Secure Remote Access Solutions

APPLIANCES | **SonicWALL SSL-VPN Series**

SonicWALL SSL-VPN 2.0 User's Guide

SONICWALL®

Using This Guide

About this Guide 5
Organization of this Guide 5
Chapter 1 Virtual Office Overview 5
Chapter 2 Using Virtual Office 5
Guide Conventions 6
Icons Used in this Manual 6

Virtual Office Overview

Virtual Office Overview 9
Accessing Virtual Office Resources 9
Browser Requirements 10
Web Management Interface Overview 11
Certificates 13

Using Virtual Office Features

Importing Certificates 15
Using One-Time Passwords 16
User Prerequisites 16
User Configuration Tasks 16
Verifying User One-Time Password Configuration 17
Troubleshooting Common Errors 18
Using NetExtender 18
User Prerequisites 18
User Configuration Tasks 19
Viewing NetExtender Information from the System Tray 29
Changing Your Password 31
Using File Shares 32
Managing Bookmarks 34
Adding Bookmarks 35
Editing Bookmarks 37
Removing Bookmarks 38

Bookmark Single Sign-On Options 38
Using Bookmarks 40
Using Remote Desktop Bookmarks. 40
Using VNC Bookmarks 41
Using FTP Bookmarks 44
Using Telnet Bookmarks 47
Using SSHv1 Bookmarks 47
Using SSHv2 Bookmarks 48
Using HTTP and HTTPS Bookmarks. 50
Using File Share Bookmarks. 50
Using Citrix Bookmarks 50
Platforms 51
Logging Out of the Virtual Office 55
Index

Using This Guide

About this Guide

Welcome to the *SonicWALL SSL-VPN User's Guide*. This manual is a user's guide. It provides information on using the SonicWALL SSL-VPN user portal called Virtual Office that allows you to create bookmarks and run services over the SonicWALL SSL-VPN security appliance.

Note Always check http://www.sonicwall.com/support/documentation.html for the latest version of this manual as well as other SonicWALL products and services documentation.

Organization of this Guide

The *SonicWALL SSL-VPN User's Guide* organization is structured into the following parts that follow the SonicWALL Web Management Interface structure. Within these parts, individual chapters correspond to SonicWALL security appliance management interface layout.

Chapter 1 Virtual Office Overview

This chapter provides an overview of new SonicWALL SSL-VPN security appliance user features, NetExtender, File Shares, services, sessions, bookmarks, and service tray menu options.

Chapter 2 Using Virtual Office

This chapter provides procedures on how to install NetExtender, working with the NetExtender system tray, displaying the NetExtender log, configuring bookmarks, and using file shares.

Guide Conventions

The following conventions used in this guide are as follows:

Convention	Use
Bold	Highlights dialog box, window, and screen names. Also highlights buttons. Also used for file names and text or values you are being instructed to type into the interface.
Italic	Indicates the name of a technical manual. Also indicates emphasis on certain words in a sentence. Also, sometimes indicates the first instance of a significant term or concept.

Icons Used in this Manual

These special messages refer to noteworthy information, and include a symbol for quick identification:

Tip Useful information about security features and configurations on your SonicWALL.

Note Important information on a feature that requires callout for special attention.

SonicWALL Technical Support

For timely resolution of technical support questions, visit SonicWALL on the Internet at *http://www.sonicwall.com/support/support.html*. Web-based resources are available to help you resolve most technical issues or contact SonicWALL Technical Support.

To contact SonicWALL telephone support, see the telephone numbers listed below:

North America Telephone Support

U.S./Canada - 888.777.1476 or +1.408.752.7819

International Telephone Support

Australia - + 1.800.35.1642

Austria - + 43(0)820.400.105

EMEA - +31(0)411.617.810

France - + 33(0)1.4933.7414

Germany - + 49(0)1805.0800.22

Hong Kong - + 1.800.93.0997

India - + 8026556828

Italy - +39(0)2.7541.9803

Japan - + 81(0)3.5460.5356

New Zealand - + 0800.446489

Singapore - + 800.110.1441

Spain - + 34(0)9137.53035

Switzerland - +41(0)1.308.3.977

UK - +44(0)1344.668.484

Note Please visit http://www.sonicwall.com/support/contact.html for the latest technical support telephone numbers.

More Information on SonicWALL Products

Contact SonicWALL, Inc. for information about SonicWALL products and services at:

Web: http://www.sonicwall.com
Email: sales@sonicwall.com
Phone: (408) 745-9600
Fax: (408)745-9300

Quick Access Work Sheet

This section should be completed by your network administrator to allow remote users SSL-VPN access.

Important Information You Need

IP Address:_____

User Name:_____

Password:_____

Domain:_____

SONICWALL
Virtual Office
Welcome to the SonicWALL Virtual Office
SonicWALL Virtual Office provides secure Internet access for remote users to log in and access private network resources via SSL-VPN technology.
User Name:
Password:
Domain:
LocalDomain
Login
Copyright © 2005 SonicWALL, Inc.

Virtual Office Overview

This chapter provides an overview of the SonicWALL SSL-VPN user portal. It also includes an introduction to the SSL-VPN and its features and applications. This chapter contains the following sections:

- "Virtual Office Overview" section on page 9
- "Browser Requirements" section on page 10
- "Web Management Interface Overview" section on page 11

Virtual Office Overview

SonicWALL SSL-VPN Virtual Office provides secure remote access to network resources, such as applications, files, intranet web sites, and email through web access interface such as Microsoft Outlook Web Access (OWA). The underlying protocol used for these sessions is SSL.

With SSL-VPN, mobile workers, telecommuters, partners, and customers can access information and applications on your intranet or extranet. What information should be accessible to the user is determined by access policies configured by the SonicWALL SSL-VPN administrator.

Accessing Virtual Office Resources

Remote network resources can be accessed in the following ways:

- **Using a standard web browser** - To access network resources, you must log into the SSL-VPN portal. Once authenticated, you may access intranet HTTP and HTTPS sites, web-based applications, and web-based email. In addition, you may upload and download files using FTP or Windows Network File Sharing. All access is performed through a standard web browser and does not require any client applications to be downloaded to remote users' machines.
- **Using Java thin-client access to corporate desktops and applications** – The SonicWALL SSL-VPN security appliance includes several Java or ActiveX thin-client programs that can be launched from within the SonicWALL SSL-VPN security appliance. Terminal Services and VNC Java clients allow remote users to access corporate servers and desktops, open files, edit and store data as if they were at the office. Terminal Services provides the ability to open individual applications and support remote sound and print services. In addition, users may access Telnet and SSH servers for SSH version 1 (SSHv1) and SSH version 2 (SSHv2), from the SSL-VPN portal.

- **Using the NetExtender SSL-VPN client** – The SonicWALL SSL-VPN security appliance includes an ActiveX-based SSL-VPN client for Window users. To connect using the SSL-VPN client, log into the portal, download the installer application and then launch the NetExtender connector to establish the SSL-VPN tunnel. Once you have set up the SSL-VPN tunnel, you can access network resources as if you were on the local network.

  With SSL-VPN releases 1.5, 2.0, and later, NetExtender is installed as a standalone client, which can be launched directly from users' computers without requiring them to log in to the SSL-VPN portal first.

For SSL-VPN to work as described in this guide, the SonicWALL SSL-VPN security appliance must be installed and configured according to the directions provided in the *SonicWALL SSL-VPN 2000 Getting Started Guide* or the *SonicWALL SSL-VPN 4000 Getting Started Guide*.

Browser Requirements

The following web browsers are supported for the web management interface and the SSL-VPN portal. Note that Java is only required for the SSL-VPN portal, not the web management interface.

Table 1 Microsoft Windows Settings

Attribute	Setting
Browser	• Internet Explorer 5.5 or higher, Mozilla 1.x, or Netscape 7.0 or higher • Opera 7.0 or higher • FireFox 1.0 or higher
Java	• Sun JRE 1.3.1 or higher
Apple MacOS X	• Browser: Safari 1.2 or higher • Java: Sun JRE 1.3.1 or higher
Unix, Linux, or BSD	• Browser: Mozilla 1.x or Netscape 7.0 or higher • Java: Sun JRE 1.31 or higher
Citrix applet	• Java: Sun JRE 1.5
Telnet, SSHv1, VNC applets	• Browser: Supports MS JVM for Internet Explorer • Java: Requires Sun JRE 1.1 or higher for other browsers
RDP5 Java applet	• Java: Sun JRE 1.2 or higher
SSHv2 applet	• Java: Sun JRE 1.4.2 or higher

To configure SonicWALL SSL-VPN software, an administrator must use a web browser with JavaScript, cookies, and SSL enabled.

Web Management Interface Overview

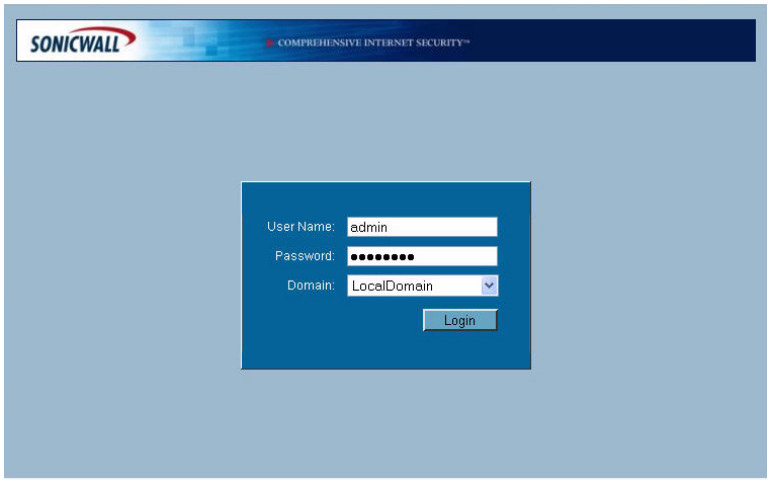
From your workstation at your remote location, launch an approved web-browser and browse to your SSL-VPN appliance at the URL provided to you by your network administrator.

Step 1 Open a Web browser and enter **https://192.168.200.1** (the default LAN management IP address) in the **Location** or **Address** field.

Step 2 A security warning may appear. Click the **Yes** button to continue.

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The security certificate has a valid name matching the name of the page you are trying to view.
Do you want to proceed?
Yes
No
View Certificate

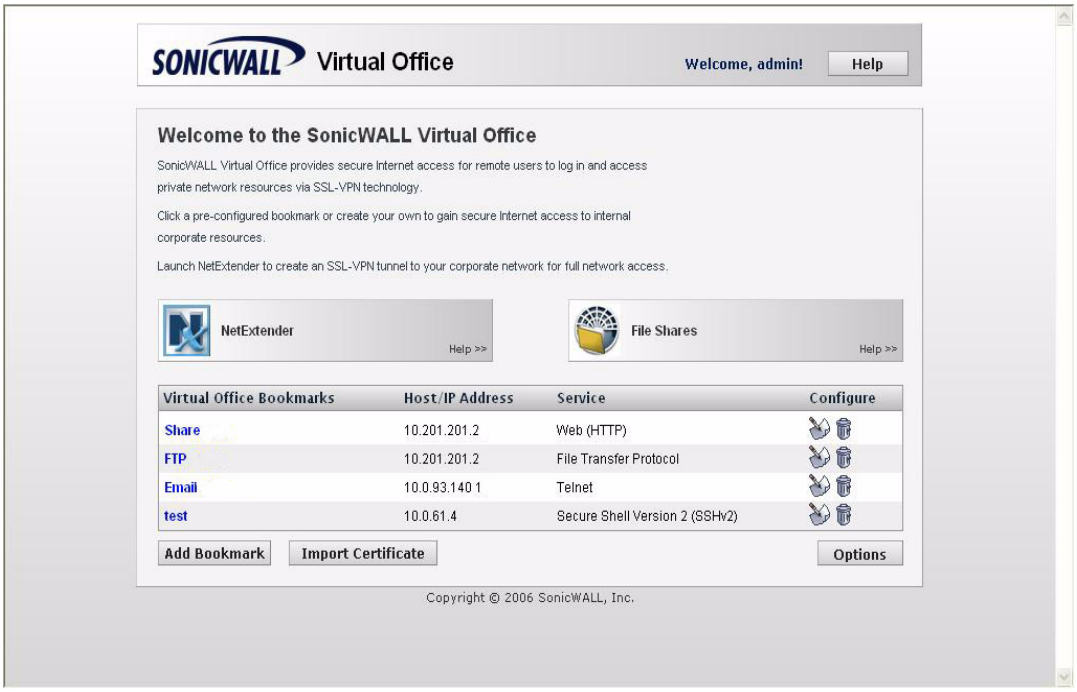
Step 3 The **SonicWALL SSL-VPN Management Interface** displays and prompts you to enter your user name and password. As a default value, enter **admin** in the **User Name** field, **password** in the **Password** field, and select a domain from the **Domain** drop-down list and click the **Login** button. Note that your administrator may have set up another login and password for you that has only user privileges.



The default page displayed is the Virtual Office home page. The default version of this page shows a SonicWALL logo, although your company's system administrator may have customized this page to contain a logo and look and feel of your company. Go to the Virtual Office Overview, page 9 to learn more about the Virtual Office home page.

Note From the Virtual Office portal home page, you cannot navigate to the administrator's environment. If you have administrator's privileges and want to enter the administrator environment, you need to go back to the login page and enter a username and password that have administrator privileges set up for them and log in again. Note that the domain is independent of the privileges set up for the user.

Logging in as a user takes you directly to Virtual Office. The Virtual Office Home page displays as shown here.



Note The Virtual Office content will vary based on the configuration of your network administrator. Some bookmarks and services described in the *SonicWALL SSL-VPN User's Guide* may not be displayed when you log into the SonicWALL SSL-VPN security appliance.

The Virtual Office consists of the nodes described in the following table.

Node	Description
File Shares	Provides access to the File Shares utility, which gives remote users with a secure Web interface access to Microsoft File Shares using the CIFS (Common Internet File System) or SMB (Server Message Block) protocols. Using a Web interface similar in style to Microsoft's familiar Network Neighborhood or My Network Places, File Shares allow users with appropriate permissions to browse network shares, rename, delete, retrieve, and upload files, and to create bookmarks for later recall.
NetExtender	Provides access to the NetExtender utility, a transparent SSL-VPN client for Windows users that allows you to run any application securely on the remote network. It acts as an IP-level mechanism provided by the virtual interface that negotiates the ActiveX component, using a Point-to-Point Protocol (PPP) adapter instance.
Bookmarks	Provides a list of available bookmarks which are objects that enable you to connect to a location or application conveniently and quickly.
Options	Provides the option to change user password and use single sign-on, if enabled by the administrator.
Online Help	Launches online help for Virtual Office.
Logout	Logs you out of the Virtual Office environment.

The Home page provides customized content and links to network resources. The Home Page may contain support contact information, VPN instructions, company news, or technical updates.

Only a web browser is required to access intranet web sites, File Shares, and FTP sites. VNC, Telnet and SSHv1 require Java. SSHv2 provides stronger encryption than SSHv1, requires SUN JRE 1.4 or 1.5 and can only connect to servers that support SSHv2. Terminal Services requires either Java or ActiveX on the client machine.

As examples of tasks you can perform and environments you can reach through Virtual Office, you can connect to:

- Intranet web or HTTPS sites – If your organization supports web-based email, such as Outlook Web Access, you can also access web-based email
- The entire network by launching the NetExtender client
- FTP servers for uploading and downloading files
- The corporate network neighborhood for file sharing
- Telnet and SSH servers
- Desktops and desktop applications using Terminal Services or VNC.
- Email servers via the NetExtender client.

The administrator determines what resources are available to users from the SonicWALL SSL-VPN Virtual Office. The administrator can create user, group, and global policies that disable access to certain machines or applications on the corporate network.

The administrator may also define bookmarks, or preconfigured links, to web sites or computers on the intranet. Additional bookmarks may be defined by the end user.

SonicWALL NetExtender is a software application that enables remote users to securely connect to the remote network. With NetExtender, remote users can virtually join the remote network. Users can mount network drives, upload and download files, and access resources in the same way as if they were on the local network.

Certificates

If the SSL-VPN gateway uses a self-signed SSL certificate for HTTPS authentication, then it is recommended to install the certificate before establishing a NetExtender connection. If you are unsure whether the certificate is self-signed or generated by a trusted root Certificate Authority, SonicWALL recommends that you import the certificate. The easiest way to import the certificate is to click the **Import Certificate** button at the bottom of the Virtual Office home page.

Using Virtual Office Features

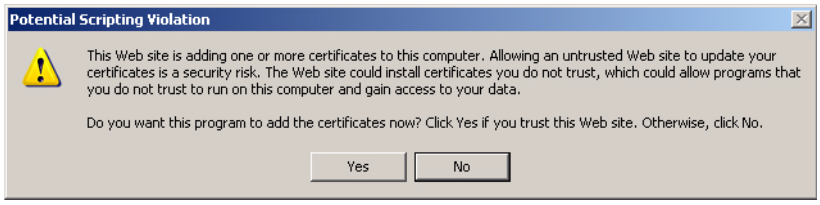
This chapter provides details on how to use the features in the SonicWALL SSL-VPN user portal, including NetExtender, configuring bookmarks, accessing services, and using file shares. This chapter contains the following sections:

- "Importing Certificates" section on page 15
- "Using One-Time Passwords" section on page 16
- "Using NetExtender" section on page 18
- "Using File Shares" section on page 32
- "Managing Bookmarks" section on page 34
- "Using Bookmarks" section on page 40
- "Logging Out of the Virtual Office" section on page 55

Importing Certificates

If the SSL-VPN gateway uses a self-signed SSL certificate for HTTPS authentication, then it is recommended to install the certificate before establishing a NetExtender connection. If you are unsure whether the certificate is self-signed or generated by a trusted root Certificate Authority, SonicWALL recommends that you import the certificate.

The easiest way to import the certificate is to click the **Import Certificate** button at the bottom of the Virtual Office home page. The following warning messages may be displayed:


Potential Scripting Violation
This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data.
Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.
Yes
No

Click **Yes**. The certificate will be imported.

Using One-Time Passwords

The following sections describe how to use one-time passwords:

- User Prerequisites, page 16
- User Configuration Tasks, page 16
- Verifying User One-Time Password Configuration, page 17
- Troubleshooting Common Errors, page 18

User Prerequisites

Users must have a user account enabled in the SSL-VPN management interface. Only users enabled by the administrator to use the One-Time Password feature will need to perform the following configuration tasks. The administrator must enable a correct email address that accessible by the user. Users cannot enable the One-Time Password feature and they must be able to access the SSL-VPN user portal, the SSL-VPN Virtual Office.

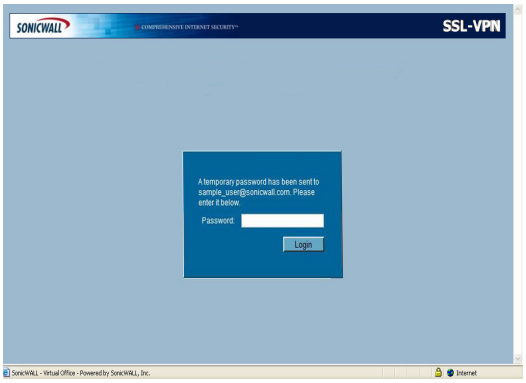
Note The One-time Password feature is supported on the SonicWALL SSL-VPN 2000 and 4000 security appliances.

User Configuration Tasks

To use the One-Time Password feature, perform the following steps:

Step 1 If you are not logged into the SSL-VPN Virtual Office user interface, open a Web browser and type the Virtual Office interface URL in the **Location** or **Address** bar and press **Enter**. Type in your user name in the **User Name** field and your password in the **Password** field, then select the appropriate domain from the **Domain** pull-down. Click **Login**.

Step 2 The prompt "A temporary password has been sent to user@email.com" will appear, displaying your pre-configured email account.



Step 3 Login to your email account to retrieve the one-time password.

Step 4 Type or paste the one-time password into the **Password:** field where prompted and click **Login**.

Step 5 You will be logged in to the Virtual Office.

Note One-time passwords are immediately deleted after a successful login, and cannot be used again. Unused one-time passwords will expire according to each user's timeout policy.

Configuring One-Time Passwords for SMS-Capable Phones

SonicWALL SSL-VPN One-Time Passwords can be configured to be sent via email directly to SMS-capable phones. Contact your cell phone service provider for further information about enabling SMS.

Below is a list of SMS email formats for selected major carriers, where 4085551212 represents a 10-digit telephone number and area code.

Note These SMS email formats are for reference only. These email formats are subject to change and may vary. You may need additional service or information from your provider before using SMS. Contact the SMS provider directly to verify these formats and for further information on SMS services, options, and capabilities.

- Verizon: 4085551212@vtext.com
- Sprint: 4085551212@messaging.sprintpcs.com
- AT&T: 4085551212@mobile.att.net
- Cingular: 4085551212@mobile.mycingular.com
- T-Mobile: 4085551212@tmomail.net
- Nextel: 4085551212@messaging.nextel.com
- Virgin Mobile: 4085551212@vmobl.com
- Qwest: 4085551212@qwestmp.com

Verifying User One-Time Password Configuration

If you are successfully logged in to Virtual Office, you have correctly used the One-Time Password feature.

If you cannot login using the One-Time Password feature, verify the following:

- Are you able to login to the Virtual Office without being prompted to check your email for a one-time password? You have not been enabled to use the One-Time Password feature.Contact your SSL-VPN administrator.
- Is your email address correct? If your email address has been entered incorrectly, contact your SSL-VPN administrator to correct it.
- Is there no email with a one-time password? Wait a few minutes and refresh your email inbox. Check your spam filter. If there is no email after several minutes, try to login again to generate a new one-time password.
- Have you accurately typed the one-time password in the correct field? Re-type or copy and paste the one-time password.

Troubleshooting Common Errors

Symptom I see an error message indicating that an email configuration is invalid, and I have verified that the One-Time Password feature is configured correctly.

Possible Cause The SonicWALL SSL-VPN One-Time Password feature does not support email servers that require passwords or other authentication. Your email server must allow anonymous access to allow the One-Time Password feature to successfully send a one-time password.

Using NetExtender

The following sections describe how to use NetExtender:

- "User Prerequisites" section on page 18
- "User Configuration Tasks" section on page 19
- "Viewing NetExtender Information from the System Tray" section on page 29

User Prerequisites

Windows clients must meet the following prerequisites in order to install NetExtender:

- Windows 2000 Professional, Windows XP Home or Professional, Windows 2000 Server or Windows 2003 Server
- Internet Explorer 5.5 and greater
- To initially install the NetExtender client, the user must be logged in to the PC with administrative privileges.
- Downloading and running scripted ActiveX files must be enabled on Internet Explorer.
- If the SSL-VPN gateway uses a self-signed SSL certificate for HTTPS authentication, then it is necessary to install the certificate before establishing a NetExtender connection. If you are unsure whether the certificate is self-signed or generated by a trusted root Certificate Authority, SonicWALL recommends that you import the certificate. The easiest way to import the certificate is to click the **Import Certificate** button at the bottom of the Virtual Office home page.

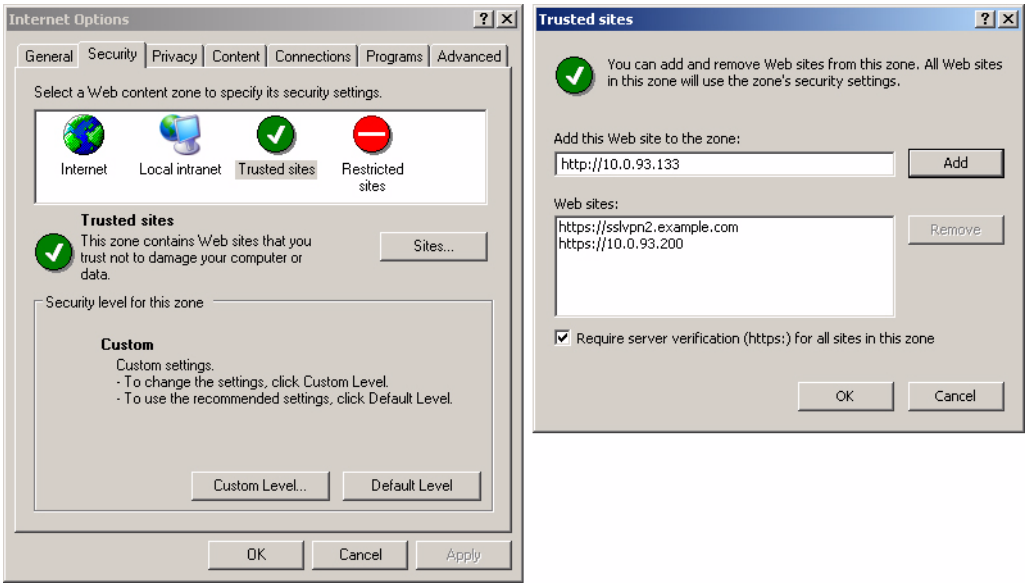
Internet Explorer Prerequisites

It is recommended that you add the URL or domain name of your SSL-VPN server to Internet Explorer's trusted sites list. This will simplify the process of installing NetExtender and logging in, by reducing the number of security warnings you will receive. To add a site to Internet Explorer's trusted sites list, complete the following procedure:

Step 1 In Internet Explorer, go to **Tools > Internet Options**.

Step 2 Click on the **Security** tab.

Step 3 Click on the **Trusted Sites** icon and click on the **Sites...** button to open the **Trusted sites** window.



Step 4 Enter the URL or domain name of your SSL-VPN server in the **Add this Web site to the zone** field and click **Add**.

Step 5 Click **OK** in the **Trusted Sites** and **Internet Options** windows.

User Configuration Tasks

SonicWALL NetExtender is a software application that enables remote users to securely connect to the remote network. With NetExtender, remote users can virtually join the remote network. Users can mount network drives, upload and download files, and access resources in the same way as if they were on the local network.

- "Installing NetExtender Using the Mozilla Firefox Browser" section on page 20
- "Installing NetExtender Using the Internet Explorer Browser" section on page 22
- "Launching NetExtender Directly from Your Computer" section on page 24
- "Configuring NetExtender Preferences" section on page 25
- "Configuring NetExtender Connection Scripts" section on page 26
- "Disconnecting NetExtender" section on page 29
- "Displaying Route Information" section on page 30
- Changing Your Password, page 31

Installing NetExtender Using the Mozilla Firefox Browser

To use NetExtender for the first time using the Mozilla Firefox browser, perform the following:

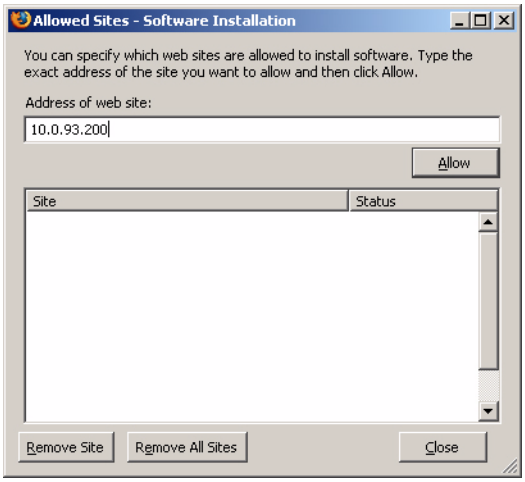
Step 1 To launch NetExtender, first log in to the SSL-VPN portal.

Step 2 Click the **NetExtender** button.

Step 3 The first time you launch NetExtender, it will automatically install the NetExtender stand-alone application on your computer. If a warning message is displayed in a yellow banner at the top of your Firefox banner, click the **Edit Options...** button.

SonicWALL - Virtual Office - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://10.0.67.89/cgi-bin/portal/
Go
To protect your computer, Firefox prevented this site (10.0.67.89) from installing software on your computer.
Edit Options...
SONICWALL Virtual Office
Welcome, joe user!
Logout
Help
Welcome to the SSL-VPN 2000
SonicWALL Virtual Office provides secure Internet access for remote users to log in and access private network resources via SSL-VPN technology.
Click a pre-configured bookmark or create your own to gain secure Internet access to internal corporate resources.
Launch NetExtender to create an SSL-VPN tunnel to your corporate network for full network access.
NetExtender
Help >>
File Shares
Help >>

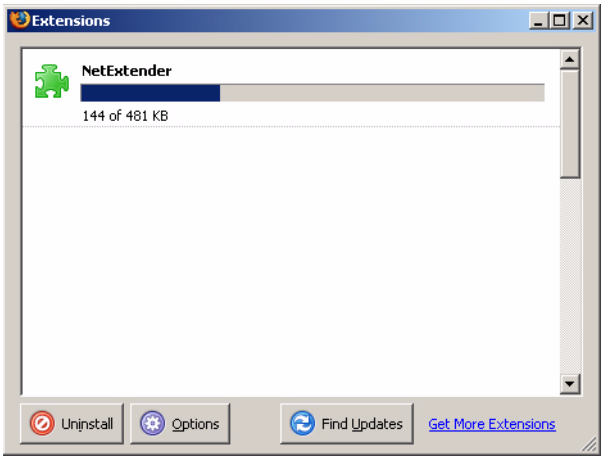
Step 4 The **Allowed Sites - Software Installation** window is displayed, with the address of the Virtual Office server in the address window. Click **Allow** to allow Virtual Office to install NetExtender, and click **Close**.


Allowed Sites - Software Installation
You can specify which web sites are allowed to install software. Type the exact address of the site you want to allow and then click Allow.
Address of web site:
10.0.93.200
Allow
Site
Status
Remove Site
Remove All Sites
Close

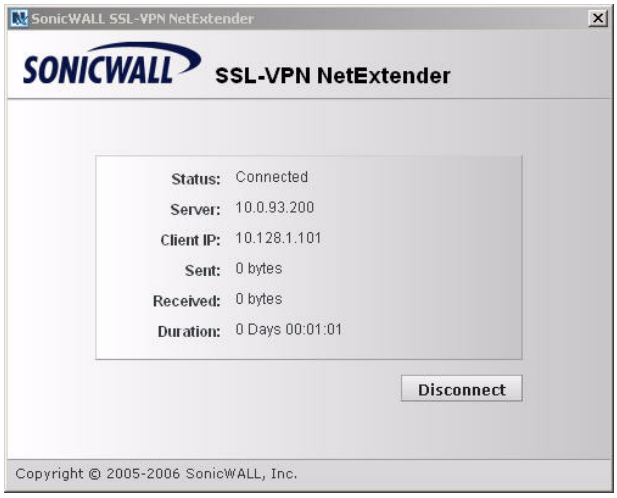
Step 5 Return to the **Virtual Office** window and click **NetExtender** again.

Step 6 The **Software Installation** window is displayed. After a five second countdown, the **Install Now** button will become active. Click it.

Step 7 NetExtender is installed as a Firefox extension.



Step 8 When NetExtender completes installing, the **NetExtender Status** window displays, indicating that NetExtender successfully connected.



By default, closing the window (clicking on the **x** icon in the upper right corner of the window) will not close the NetExtender session, but will minimize it to the system tray for continued operation. To configure NetExtender to disconnect when you close the NetExtender window, see the "Configuring NetExtender Preferences" section on page 25.

Step 9 Review the following table to understand the fields in the **NetExtender Status** window.

Field	Description
Status	Indicates what operating state the NetExtender client is in, either Connected or Disconnected.
Server	Indicates the name of the server to which the NetExtender client is connected.
Client IP	Indicates the IP address assigned to the NetExtender client.
Sent	Indicates the amount of traffic the NetExtender client has transmitted since initial connection.

Field	Description
Received	Indicates the amount of traffic the NetExtender client has received since initial connection.
Duration	The amount of time the NetExtender has been connected, expressed as days, hours, minutes, and seconds.

Step 10 Additionally, a balloon icon in the system tray appears, indicating NetExtender has successfully installed.

Step 11 The NetExtender icon is displayed in the task bar.

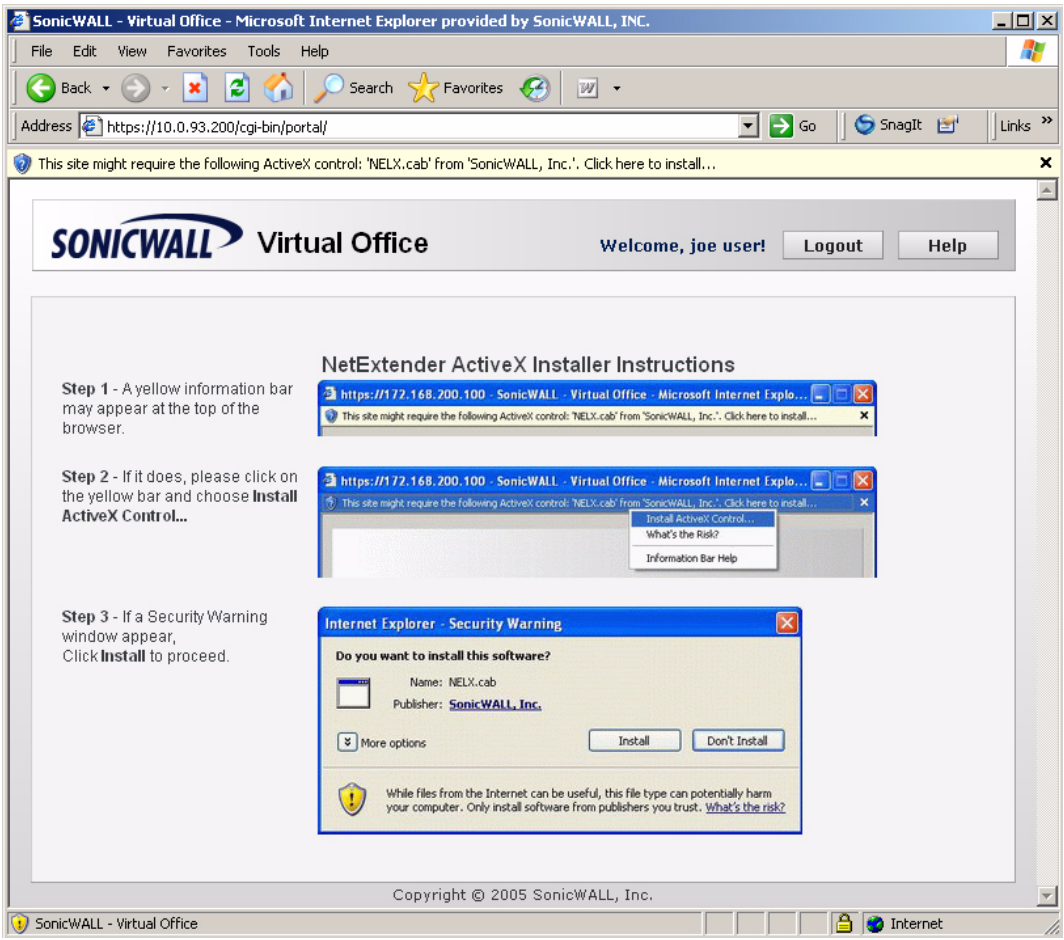
Installing NetExtender Using the Internet Explorer Browser

To use NetExtender for the first time using the Internet Explorer browser, perform the following:

Step 1 To launch NetExtender, first log in to the SSL-VPN portal.

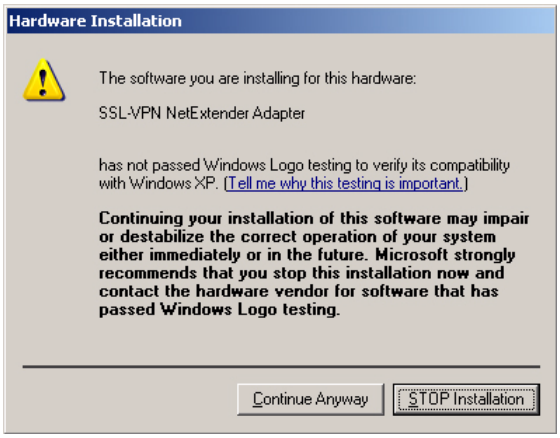
Step 2 Click the **NetExtender** button.

Step 3 The first time you launch NetExtender, it will automatically install the NetExtender stand-alone application on your computer. The NetExtender installer window opens.

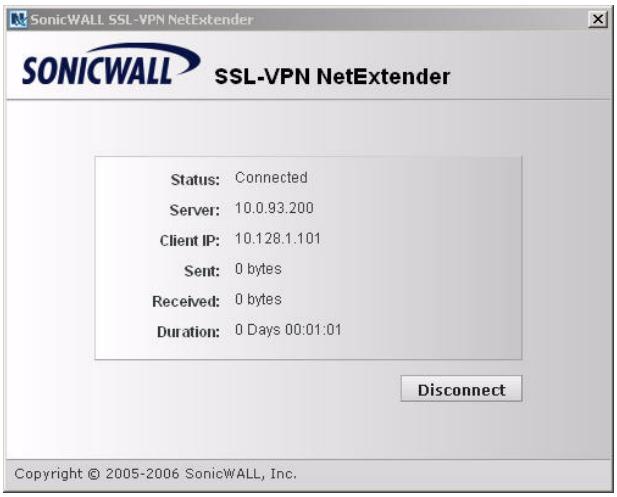

SonicWALL - Virtual Office - Microsoft Internet Explorer provided by SonicWALL, INC.
File Edit View Favorites Tools Help
Back Search Favorites
Address https://10.0.93.200/cgi-bin/portal/
Go SnagIt Links
This site might require the following ActiveX control: 'NELX.cab' from 'SonicWALL, Inc.'. Click here to install...
SONICWALL Virtual Office
Welcome, joe user!
Logout
Help
NetExtender ActiveX Installer Instructions
Step 1 - A yellow information bar may appear at the top of the browser.
Step 2 - If it does, please click on the yellow bar and choose Install ActiveX Control...
Install ActiveX Control...
What's the Risk?
Information Bar Help
Step 3 - If a Security Warning window appear, Click Install to proceed.
Internet Explorer - Security Warning
Do you want to install this software?
Name: NELX.cab
Publisher: SonicWALL, Inc.
More options
Install
Don't Install
While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?
Copyright © 2005 SonicWALL, Inc.
SonicWALL - Virtual Office
Internet

Step 4 If an older version of NetExtender is installed on the computer, the NetExtender launcher will remove the old version and then install the new version.

Step 5 If the following warning message is displayed, click **Continue Anyway**. SonicWALL testing has verified that NetExtender is fully compatible with Windows XP and 2000.


Hardware Installation
The software you are installing for this hardware:
SSL-VPN NetExtender Adapter
has not passed Windows Logo testing to verify its compatibility with Windows XP. (Tell me why this testing is important.)
Continuing your installation of this software may impair or destabilize the correct operation of your system either immediately or in the future. Microsoft strongly recommends that you stop this installation now and contact the hardware vendor for software that has passed Windows Logo testing.
Continue Anyway
STOP Installation

Step 6 When NetExtender completes installing, the **NetExtender Status** window displays, indicating that NetExtender successfully connected.



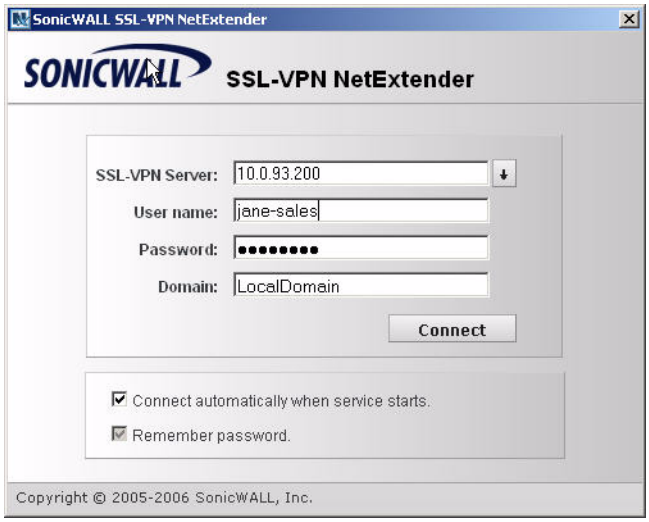
Launching NetExtender Directly from Your Computer

In SonicWALL SSL-VPN releases 1.5, 2.0, and later, you can launch NetExtender directly from your computer without first navigating to the SSL-VPN portal. To launch NetExtender, complete the following procedure:

Step 1 Navigate to **Start > All Programs**.

Step 2 Select the **SonicWALL SSL-VPN NetExtender** folder, and then click on **SonicWALL SSL-VPN NetExtender**. The NetExtender login window is displayed.

Step 3 The IP address of the last SSL-VPN server you connected to is displayed in the **SSL-VPN Server** field. To display a list of recent SSL-VPN servers you have connected to, click on the arrow.



Step 4 Enter your username and password.

Step 5 The last domain you connected to is displayed in the **Domain** field.

Step 6 Check the **Connect automatically when service starts** checkbox to have NetExtender automatically connect when you log on to Windows.

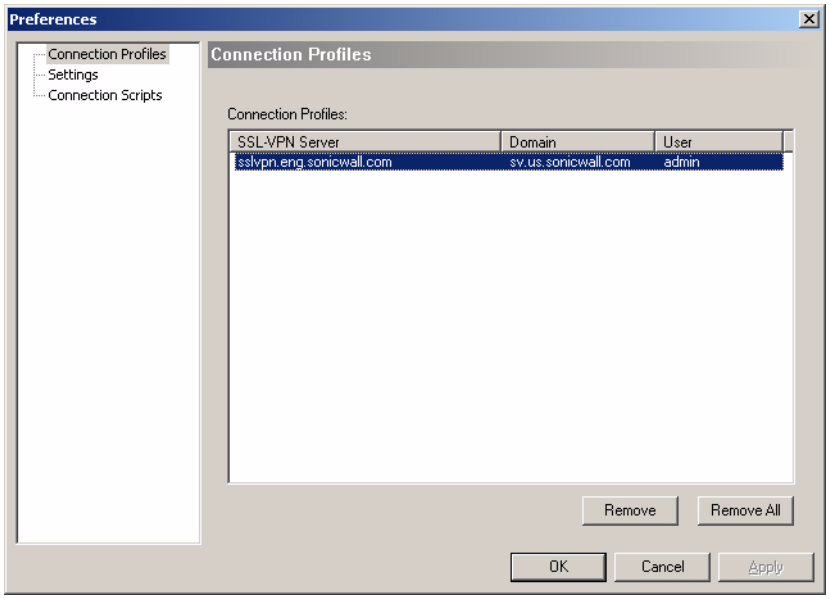
Step 7 Check the **Remember password** checkbox to preserve your password. This can be a security risk and should not be enabled if there is a chance that other people could use your computer to access sensitive information on the network.

Configuring NetExtender Preferences

Complete the following procedure to configure NetExtender preferences:

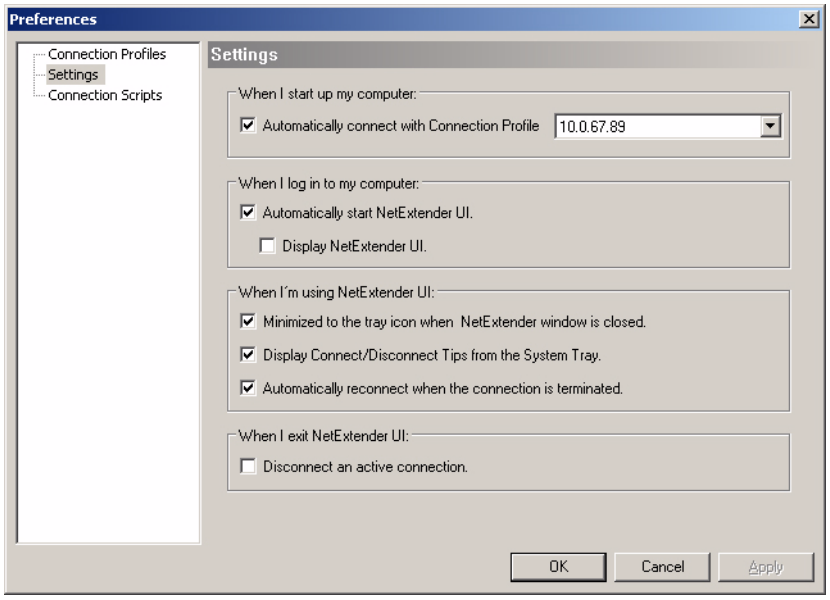
Step 1 Right click on the icon in the task bar and click on **Preferences...** The NetExtender Preferences window is displayed.

Step 2 The **Connection Profiles** tab displays the SSL-VPN connection profiles you have used, including the IP address of the SSL-VPN server, the domain, and the username.



Step 3 To delete a profile, highlight it by clicking on it and then click the **Remove** buttons. Click the **Remove All** buttons to delete all connection profiles.

Step 4 The **Settings** tab allows you to customize the behavior of NetExtender.



Step 5 To instruct NetExtender to automatically connect to an SSL-VPN server when NetExtender is launched, check the **Automatically Connect with Connection Profile** checkbox and select the IP address of the server from the pull-down menu of SSL-VPN servers.

Step 6 To instruct NetExtender to automatically start when you log on to Windows, check the **Automatically start NetExtender UI** checkbox in the **When I log in to my computer** section.

Step 7 To instruct NetExtender to display the NetExtender window when it connects after Windows logs on, check the **Display NetExtender UI** checkbox.

Step 8 Check the **Minimize to the tray icon when NetExtender window is closed** checkbox in the **When I'm Using NetExtender UI** section to have the NetExtender icon displayed in the system tray when you close the NetExtender window.

Step 9 To instruct NetExtender to disconnect when you close the NetExtender window, check the **Disconnect an Active Connection** checkbox in the **When I exit NetExtender UI** section.

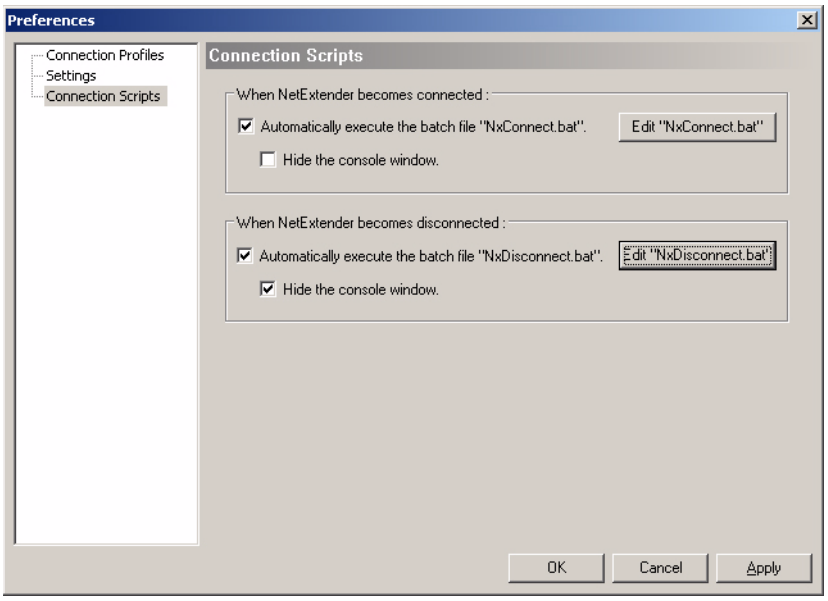
Step 10 Select the **Disconnect an active connection** checkbox in the **When I exit NetExtender UI section** to have NetExtender disconnect when you close the NetExtender window.

Configuring NetExtender Connection Scripts

SonicWALL SSL-VPN release 2.0 provides users with the ability to run batch file scripts when NetExtender connects and disconnects. The scripts can be used to map or disconnect network drives and printers, launch applications, or open files or websites. To configure NetExtender Connection Scripts, perform the following tasks.

Step 1 Right click on the icon in the task bar and click on **Preferences...** The NetExtender Preferences window is displayed.

Step 2 Click on **Connection Scripts**.



Step 3 To enable the script that runs when NetExtender connects, select the **Automatically execute the batch file "NxConnect.bat"** checkbox.

Step 4 To enable the script that runs when NetExtender disconnects, select the **Automatically execute the batch file "NxDisconnect.bat"** checkbox.

Step 5 To hide either of the console windows, select the appropriate **Hide the console window** checkbox. If this checkbox is not selected, the DOS console window will remain open while the script runs.

Configuring Batch File Commands

NetExtender Connection Scripts can support any valid commands. For more information on batch files, see the following Wikipedia entry: http://en.wikipedia.org/wiki/.bat. The following tasks provide an introduction to some commonly used batch file commands.

Step 1 To configure the script that runs when NetExtender connects, click the **Edit "NxConnect.bat"** button. The NxConnect.bat file is displayed.

Step 2 To configure the script that runs when NetExtender disconnects, click the **Edit "NxDisconnect.bat"** button. The NxConnect.bat file is displayed.

Step 3 By default, the **NxConnect.bat** file contains examples of commands that can be configured, but no actual commands. Too add commands, scroll to the bottom of the file.

Step 4 To map a network drive, enter a command in the following format:

net use *drive-letter\\server\share password* **/user:***Domain\name*

For example to if the drive letter is **z**, the server name is **engineering**, the share is **docs**, the password is **1234**, the user's domain is **eng** and the username is **admin**, the command would be the following:

net use z\\engineering\docs 1234 /user:eng\admin

Step 5 To disconnect a network drive, enter a command in the following format:

net use *drive-letter***: /delete**

For example, to disconnect network drive z, enter the following command:

net use z: /delete

Step 6 To map a network printer, enter a command in the following format:

net use LPT1 *ServerName**PrinterNa*me **/user:***Domain**name*

For example, if the server name is **engineering**, the printer name is **color-print1**, the domain name is **eng**, and the username is admin, the command would be the following:

net use LPT1 \\engineering\color-print1 /user:eng\admin

Step 7 To disconnect a network printer, enter a command in the following format:

net use LPT1 /delete

Step 8 To launch an application enter a command in the following format:

C:*Path-to-Application**Application.exe*

Step 9 For example, to launch Microsoft Outlook, enter the following command:

C:\Program Files\Microsoft Office\OFFICE11\outlook.exe

Step 10 To open a website in your default browser, enter a command in the following format:

start http://*www.website.com*

Step 11 To open a file on your computer, enter a command in the following format:

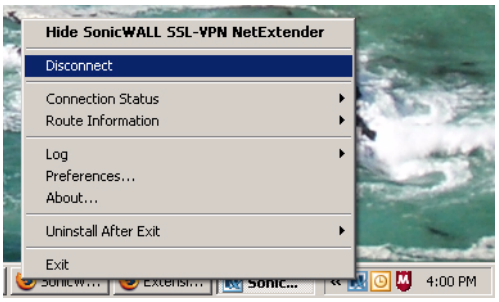
C:\Path-to-file\myFile.doc

Step 12 When you have finished editing the scripts, save the file and close it.

Disconnecting NetExtender

To disconnect NetExtender, perform the following steps:

Step 1 Right click on the NetExtender icon in the system tray to display the NetExtender icon menu.



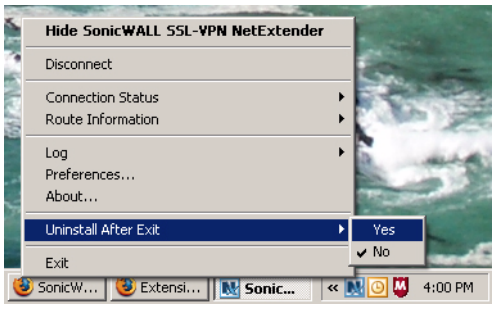
Step 2 Click the **Disconnect** option.

Step 3 Wait several seconds. The NetExtender session disconnects.

You can also disconnect by double clicking on the NetExtender icon to open the **NetExtender** window and then clicking the **Disconnect** button.

Instruct NetExtender to Uninstall After Exit

To have NetExtender automatically uninstall when you exit your NetExtender session, right click on the NetExtender icon, select **Uninstall After Exit**, and click **Yes**.



Uninstalling NetExtender

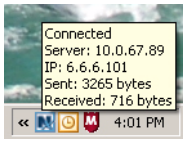
The NetExtender utility is automatically installed on your computer. To remove NetExtender, click on **Start > All Programs**, click on **SonicWALL SSL-VPN NetExtender**, and then click on **Uninstall**.

Viewing NetExtender Information from the System Tray

The following sections describe the NetExtender information that can be displayed from the system tray, including connection details, the NetExtender log, and route information.

Displaying Connection Information

You can display connection information by mousing over the NetExtender icon in the system tray. You can also display this information by right clicking on the NetExtender icon and clicking on **System Status**.



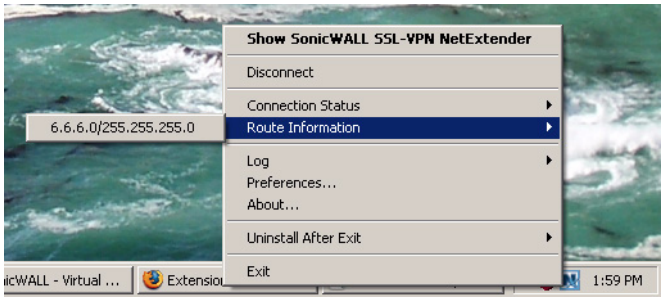
Viewing the NetExtender Log

The NetExtender log contains details about session establishment, termination, and other events. To display the NetExtender log, right click on the NetExtender icon and click on **Log** and then **View Log...** in the system tray menu.The log is stored as the file NetExtender.dbg in the directory C:\Program Files\SonicWALL\SSL-VPN\NetExtender.

To clear the contents of the NetExtender log, click on **Log** and then **Clear Log** in the system tray menu.

Displaying Route Information

To display the routes that NetExtender has installed on your system, right click on the NetExtender icon and click the **Route Information** option in the system tray menu. The system tray menu displays all installed routes and their associated subnet masks.



Changing Your Password

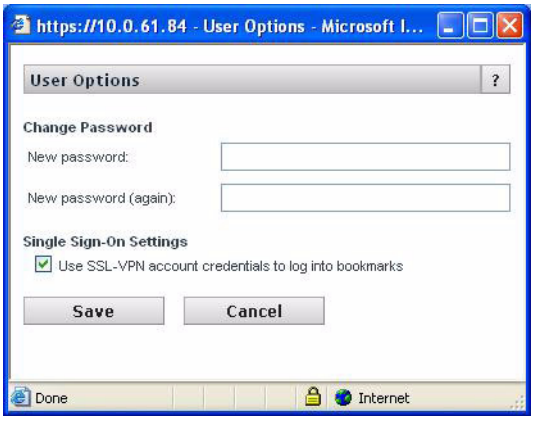
You can change your password using the **Options** button on the main Virtual Office page. To change your password, perform the following tasks:

Step 1 Click the **Options** button. The **User Options** page displays.

Figure 4:1 Virtual Office

SONICWALL Virtual Office
Welcome, admin!
Help
Welcome to the SonicWALL Virtual Office
SonicWALL Virtual Office provides secure Internet access for remote users to log in and access private network resources via SSL-VPN technology.
Click a pre-configured bookmark or create your own to gain secure Internet access to internal corporate resources.
Launch NetExtender to create an SSL-VPN tunnel to your corporate network for full network access.
NetExtender
Help >>
File Shares
Help >>
Virtual Office Bookmarks
Host/IP Address
Service
Configure
Sharepoint
10.201.201.20
Web (HTTP)
FTP Eagle
10.201.201.20
File Transfer Protocol
Add Bookmark
Import Certificate
Options
Copyright © 2006 SonicWALL, Inc.

Figure 4:2 User Options



Step 2 Type a new password in the **New Password** field.

Step 3 Re-type the new password in the **New Password (again)** field.

Step 4 Click **Save**.

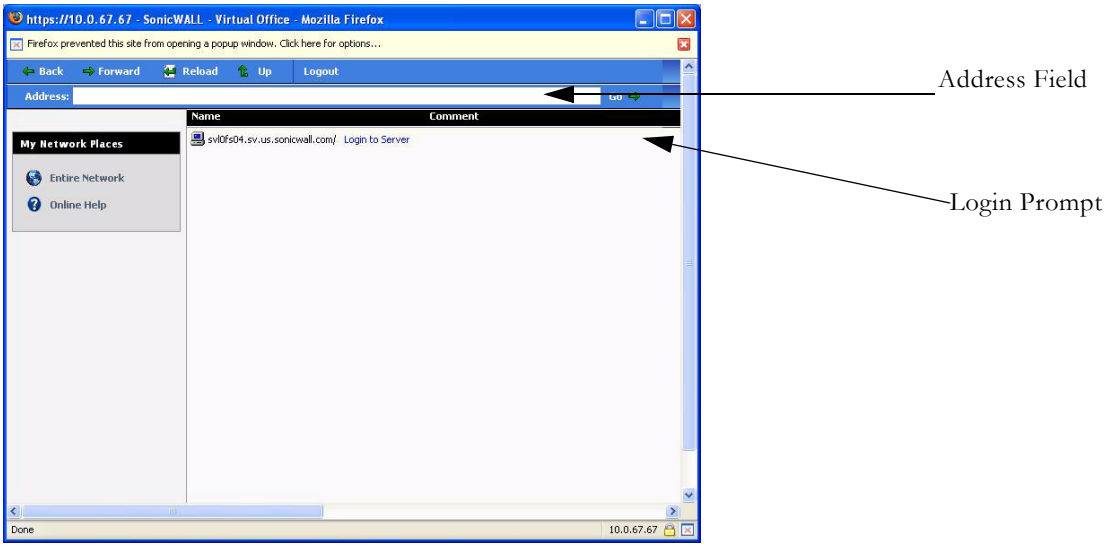
Using File Shares

File shares provide remote users with a secure Web interface to Microsoft File Shares using the CIFS (Common Internet File System) or SMB (Server Message Block) protocols. Using a Web interface similar in style to Microsoft's familiar Network Neighborhood or My Network Places, File Shares allow users with appropriate permissions to browse network shares, rename, delete, retrieve, and upload files, and to create bookmarks for later recall.

Note The server can be specified either by name or by IP address, for example, **moosedc** or **10.50.165.2**. For names to work, it is necessary that DNS and or WINS be properly configured by the administrator on the SSL-VPN appliance to be able to resolve host names.

To create a file share, perform the following steps:

Step 1 Click on the File Shares button. Virtual Office displays a dialog box that provides a hot link to a login prompt.



Note Pop-up window blockers may prevent File Shares from functioning properly. Configure your browser to allow pop-up windows on the SSL-VPN portal site.

Step 2 To specify a new share path (as an example, **moosedc**) in the **Address** field. You need to precede the share name with two back slashes. For example: **file-directory01.example.com**.

Step 3 To connect to a pre-existing file share, click the **Login to Server** link next to the file share name.

Step 4 Click the **go** prompt to display the **Enter Network Password** dialog box.

Step 5 Type a valid username in the User Name field and a valid password in the Password field and click **Login**.

Step 6 Virtual Office displays the home File Share screen that you have specified, displaying folders on the network to which you can navigate.

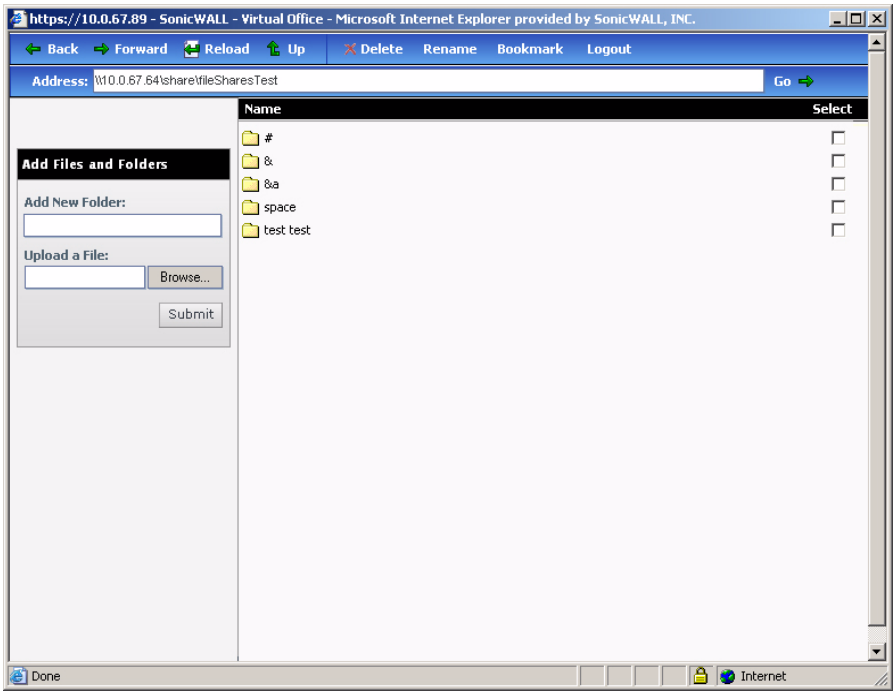


Table 1 describes the controls at the top of the File Share window.

Table 1 File Share Controls

Button	Description
Back	Navigate to the previous File Share location.
Forward	Navigates forward to the previous File Share location after you have pressed the **Back** button.
Reload	Reloads the current folder to display any changes.
Up	Navigates
Delete	Deletes the selected folders and files. Select items by checking the checkbox next to their name under the **Select** column.
Rename	Renames the selected folders and files. Select items by checking the checkbox next to their name under the **Select** column.

Table 1 File Share Controls

Button	Description
Bookmark	Creates a new bookmark to the current File Share location.
Logout	Logout of the File Share service.

Step 7 You can now navigate the folders and files in the File Share as you would through Windows Explorer or other file management systems.

Step 8 To add a new folder in the current File Share location, type the name of the folder in the **Add New Folder:** field and click **Submit**.

Step 9 To add a file in the current File Share location, click the **Browse...** button. Navigate to the location of the file on your computer in the **Choose file** window that opens, select the file and click **ok**, and then click **Submit** in the File Share window.

Managing Bookmarks

Bookmarks are objects that enable you to connect to a location or application conveniently and quickly. The Virtual Office Bookmark system allows bookmarks to be created at the group and user levels. The administrator can create both group and user bookmarks which will apply to applicable users while individual users can create only personal (user-level) bookmarks.

Since bookmarks are stored within the security appliance's local configuration files, it is necessary for group and user bookmarks to be correlated to defined group and user entities. When working with local groups and users (LocalDomain), this is automated since the administrator must manually define the groups and users on the device. Similarly, when working with external groups (not LocalDomain), the correlation is automated since creating an external domain creates a corresponding local group.

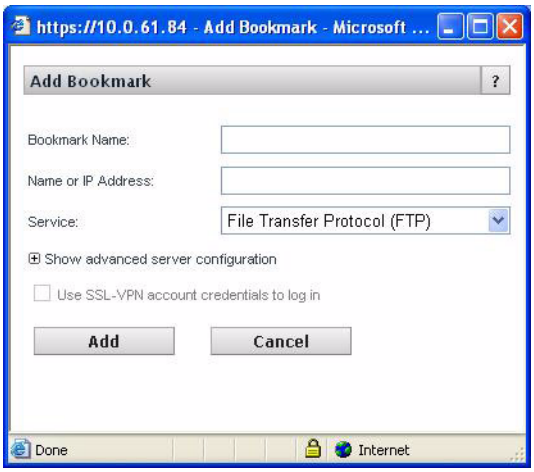
However, when working with external users, a local user entity must exist so that any user-created (personal) bookmarks can be stored within the SSL-VPN's configuration files. The need to store bookmarks on the SSL-VPN itself is because LDAP, RADIUS, and NT authentication external domains do not provide a direct facility to store such information as bookmarks.

Rather than requiring administrators to manually create local users for external domain users wishing to use personal bookmarks, SonicWALL SSL-VPN automatically creates a corresponding local user entity when an external domain user logs in to the Virtual Office.

Adding Bookmarks

Bookmarks provide a convenient way for you to access web, FTP, or other services on the remote network that you will connect to frequently. To define bookmarks, perform the following:

Step 1 From the Virtual Office window, click **Add Bookmark** in the Bookmarks table. An Add Bookmark window will be displayed.



Step 2 Enter a descriptive name in the **Bookmark Name** field.

Step 3 Enter the domain name or the IP address of a host machine on the LAN in the **Name or IP Address** field.

Step 4 Select the service type in the Service menu. You can select from the following services:

- Terminal Services (RDP5 - ActiveX)
- Terminal Services (RDP5 - Java)
- Virtual Network Computing (VNC)
- File Transfer Protocol (FTP)
- Telnet
- Secure Shell version 1 (SSHv1)
- Secure Shell version 2 (SSHv2)
- Web (HTTP)
- Secure Web (HTTPS)
- File Share (CIFS/SMB)
- Citrix Portal (Citrix)

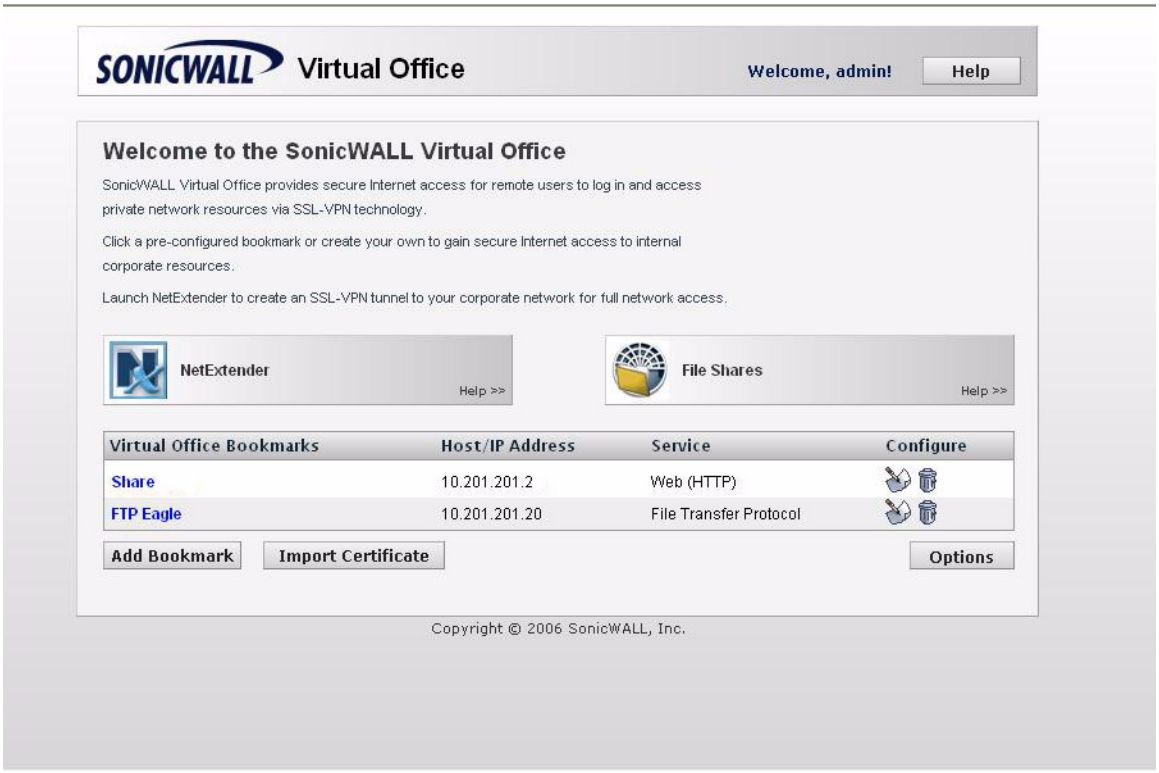
Step 5 For Citrix bookmarks, you can optionally designate that it be a secure Citrix connection by checking the **HTTPS Mode** checkbox.

Step 6 For RDP5 - ActiveX, RDP5 - Java and FTP, check the box next to **Use SSL-VPN account credentials to log in** to use SSL-VPN account credentials to log in. Leave the box unchecked to use custom credentials for each bookmark login.

Step 7 For SSHv2, you must have SUN JRE 1.4 or 1.5 and must be connecting to a server that supports SSHv2.

Step 8 Click **Add** to add the bookmark.

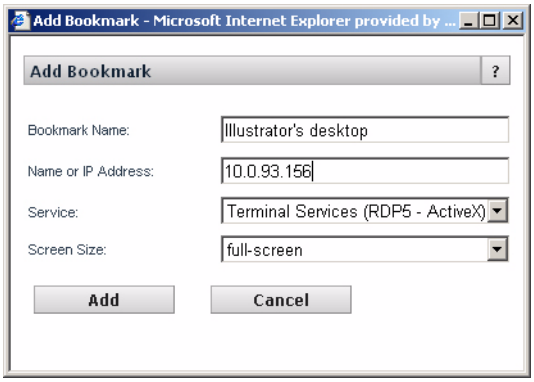
Once the configuration has been updated, the new bookmark will be displayed in the Bookmarks table. Click on a bookmark description to go to the bookmark location that you have defined.


SONICWALL Virtual Office
Welcome, admin!
Help
Welcome to the SonicWALL Virtual Office
SonicWALL Virtual Office provides secure Internet access for remote users to log in and access private network resources via SSL-VPN technology.
Click a pre-configured bookmark or create your own to gain secure Internet access to internal corporate resources.
Launch NetExtender to create an SSL-VPN tunnel to your corporate network for full network access.
NetExtender
Help >>
File Shares
Help >>
Virtual Office Bookmarks
Host/IP Address
Service
Configure
Share
10.201.201.2
Web (HTTP)
FTP Eagle
10.201.201.20
File Transfer Protocol
Add Bookmark
Import Certificate
Options
Copyright © 2006 SonicWALL, Inc.

Configuring RDP Bookmarks

For RDP Terminal Services bookmarks, there are two additional options.

Step 1 Select the resolution for the RDP window. It is advised that you select a size equal to or smaller than your current desktop screen size. ActiveX RDP bookmarks also have a **full-screen** option that will display the RDP window in full screen mode. To toggle from the RDP window back to your desktop, press **Alt-Tab**.



Tip The ActiveX client is only supported on the Internet Explorer browser, while the Java client is supported on all platforms and browsers that are compatible with SonicWALL SSL-VPN.

Step 2 To have the RDP session launch an application when the bookmark is initiated, enter the path to the application in the **Application and Path (optional):** field. For example, **C:\Program Files\Example\app.exe**.

Determining the Remote Computer's Full Name or IP Address

Complete the following steps to determine the full name of the computer the RDP bookmark is pointing to:

Step 1 Right click on the **My Computer** icon on the desktop of the remote computer, and select **Properties**.

Step 2 Click the **Remote** tab.

Step 3 The full computer name will be listed under Remote Desktop.

Complete the following steps to determine the IP address of your computer.

Step 1 In the Windows **Start** menu on the remote computer, navigate to **Run...**

Step 2 Type **CMD** to open the command interpreter and press **OK**.

Step 3 Type **IPconfig**. The IP address of your computer is displayed.

Configuring Remote Desktop Access on the Remote Computer

Complete the following steps to allow remote desktop access to the computer that is the target of the RDP bookmark:

Step 1 Right click on the **My Computer** icon on the desktop, and select **Properties**.

Step 2 Click the **Remote** tab.

Step 3 Check the box next to **Allow users to connect remotely to this computer**

Step 4 Click **Apply.**

Step 5 Click **OK**.

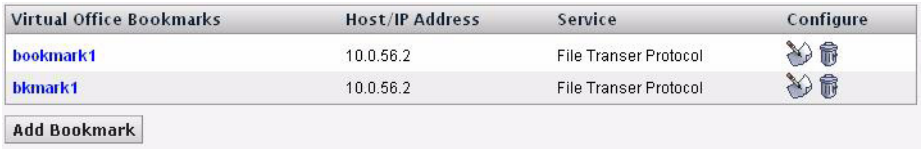
Editing Bookmarks

You can change the IP address or domain name as well as the service associated with an existing bookmark.

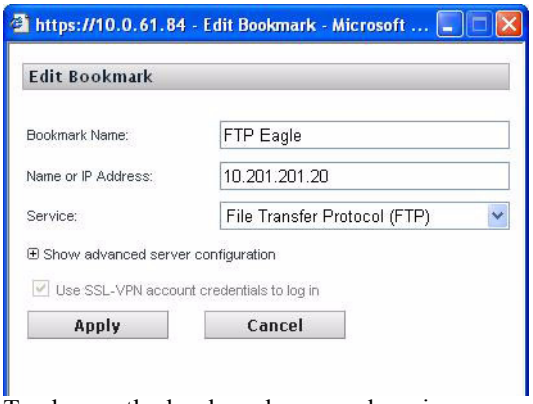
Note Only user-created Bookmarks can be edited or deleted by the user. Global Bookmarks pre-defined by the administrator can not be edited or deleted.

To edit a bookmark to change its name or associated IP address, perform the following steps:

Step 1 Identify a bookmark in the Bookmarks list for which you want to change an IP address or domain name.



Step 2 In the Bookmarks list, click on the Configure icon for an existing bookmark. The **Edit Bookmark** dialog box displays.



Step 3 To change the bookmark name, domain name or IP address of the bookmark, edit the names in the **Bookmark Name** or **Name or IP Address** fields.

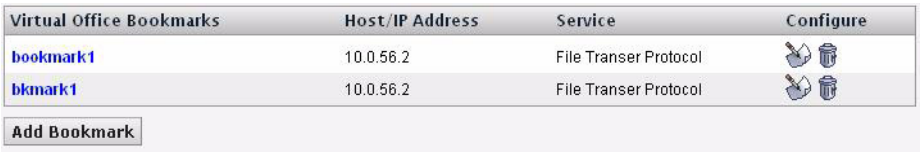
Step 4 To change the service, select a new service from the pull-down menu.

Step 5 Click **Apply**. The Virtual Office home page displays with the new IP address or domain name.

Removing Bookmarks

To remove a bookmark, perform the following steps:

Step 1 Identify a bookmark in the Bookmarks list that you want to remove.



Step 2 In the Bookmarks list, click on the trash icon for the bookmark you want to remove. The bookmark disappears from the Bookmarks list.

Caution No warning message is displayed after you click the trash icon. The bookmark will be deleted immediately.

Bookmark Single Sign-On Options

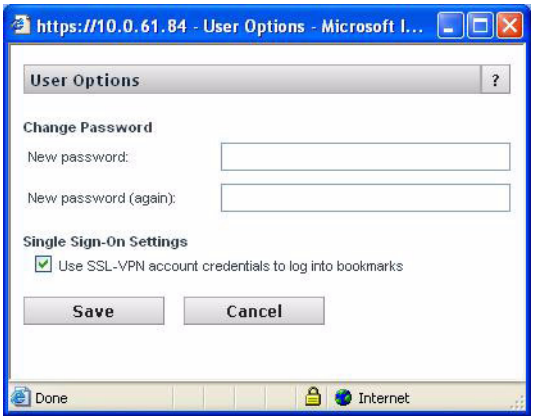
You can configure single sign-on using the **Options** button on the main Virtual Office page. SSO settings will be enabled only if the administrator has configured user- controlled single sign-on (SSO). To configure SSO bookmark options, perform the following tasks:

Step 1 Click the **Options** button. The **User Options** page displays.

Figure 4:3 Virtual Office

SONICWALL Virtual Office
Welcome, admin!
Help
Welcome to the SonicWALL Virtual Office
SonicWALL Virtual Office provides secure Internet access for remote users to log in and access private network resources via SSL-VPN technology.
Click a pre-configured bookmark or create your own to gain secure Internet access to internal corporate resources.
Launch NetExtender to create an SSL-VPN tunnel to your corporate network for full network access.
NetExtender
Help >>
File Shares
Help >>
Virtual Office Bookmarks
Host/IP Address
Service
Configure
Sharepoint
10.201.201.20
Web (HTTP)
FTP Eagle
10.201.201.20
File Transfer Protocol
Add Bookmark
Import Certificate
Options
Copyright © 2006 SonicWALL, Inc.

Figure 4:4 User Options



Step 2 Under **Single Sign-On Settings**, check the **Use SSL-VPN account credentials to log into bookmarks** to enable SSO for bookmarks. Leave the box unchecked if you do not want to use SSO for bookmarks.

Step 3 Click **Save** to save your changes.

Note Fileshares will use the configured domain name of which the user is a member to supply to the backend server. HTTP, HTTPS, FTP, RDP5 - ActiveX, RDP5- Java will supply the username and password that was used to login. If the server is expecting a domain-prefixed username, SSO will fail. In some cases, a default domain can be specified at the server to allow SSO to succeed.

Using Bookmarks

The following sections describe how to use the various types of bookmarks:

- "Using Remote Desktop Bookmarks" section on page 40
- "Using VNC Bookmarks" section on page 41
- "Using FTP Bookmarks" section on page 44
- "Using Telnet Bookmarks" section on page 47
- "Using SSHv1 Bookmarks" section on page 47
- "Using SSHv2 Bookmarks" section on page 48
- "Using HTTP and HTTPS Bookmarks" section on page 50
- "Using File Share Bookmarks" section on page 50
- "Using Citrix Bookmarks" section on page 50

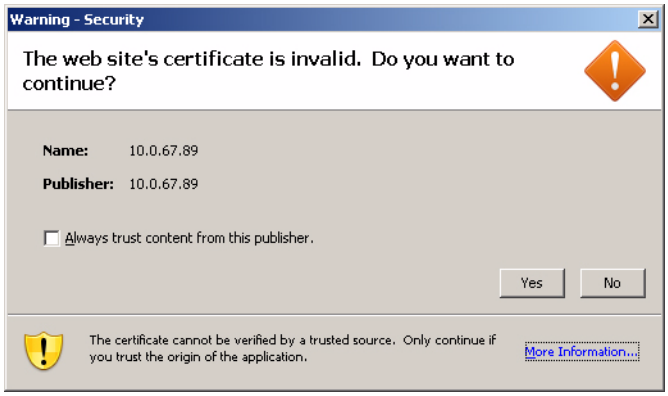
Using Remote Desktop Bookmarks

Remote Desktop Protocol (RDP) bookmarks enable you to establish remote connections with a specified desktop. SSL-VPN releases 1.5, 2.0, and later support the RDP5 standard with both Java and an ActiveX clients. RDP5 ActiveX can only be used through Internet Explorer, while RDP5 Java can be run on any platform and browser that supports the SonicWALL SSL-VPN. The basic functionality of the two clients is the same; however, the ActiveX client supports the following features that the Java client does not:

- Full-screen mode
- Remote printing
- Drive mapping
- Multiple simultaneous RDP sessions

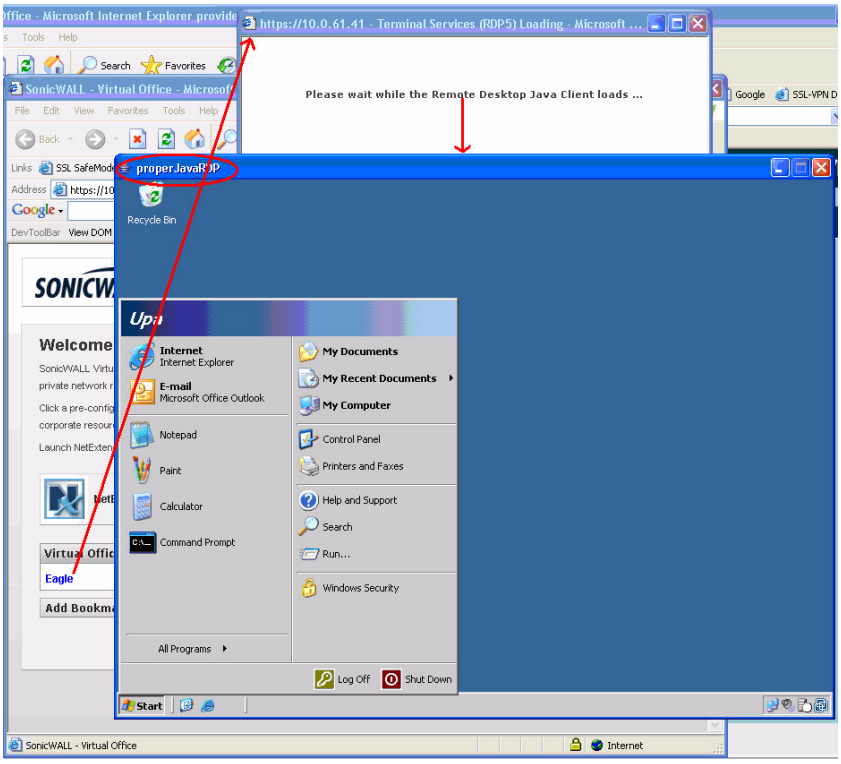
Tip To terminate your remote desktop session, be sure to log off from the Terminal Server session. If you wish to suspend the Terminal Server session (so that it can be resumed later) you may simply close the remote desktop window.

Step 1 Click on the **RDP** bookmark. Continue through any warning screens that display by clicking **Yes** or **Ok**.


Warning - Security
The web site's certificate is invalid. Do you want to continue?
Name: 10.0.67.89
Publisher: 10.0.67.89
Always trust content from this publisher.
Yes
No
The certificate cannot be verified by a trusted source. Only continue if you trust the origin of the application.
More Information...

Step 2 Enter your username and password at the login screen and select the proper domain name from the pull-down menu.

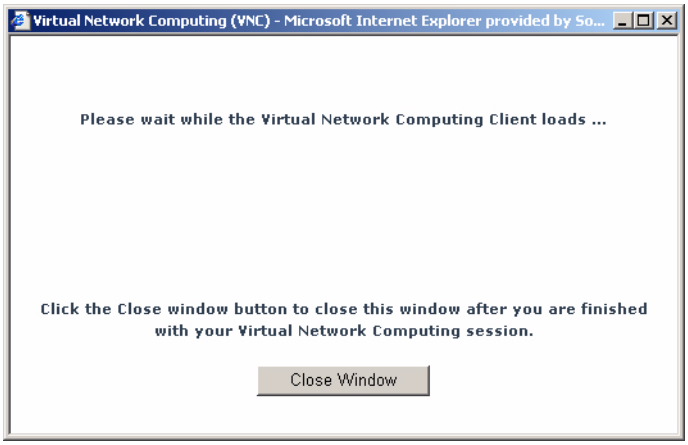
Step 3 A window is displayed indicating that the Remote Desktop Client is loading. The remote desktop then loads in its own windows. You can now access all of the applications and files on the remote computer.



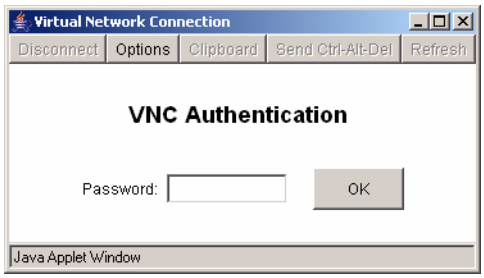
Using VNC Bookmarks

Step 1 Click the VNC bookmark. The following window is displayed while the VNC client is loading.

Note VNC can have a port designation if the service is funning on a different port.


Virtual Network Computing (VNC) - Microsoft Internet Explorer provided by So...
Please wait while the Virtual Network Computing Client loads ...
Click the Close window button to close this window after you are finished with your Virtual Network Computing session.
Close Window

Step 2 When the VNC client has loaded, you will be prompted to enter your password in the **VNC Authentication** window.



Step 3 To configure VNC options, click the **Options** button. The **Options** window is displayed.

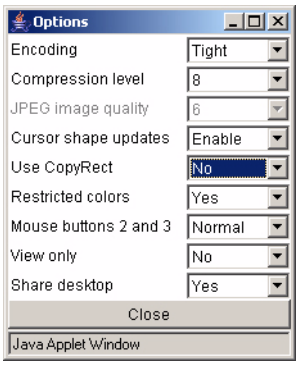


Table 2 describes the options that can be configured for VNC.

Table 2 VNC Options

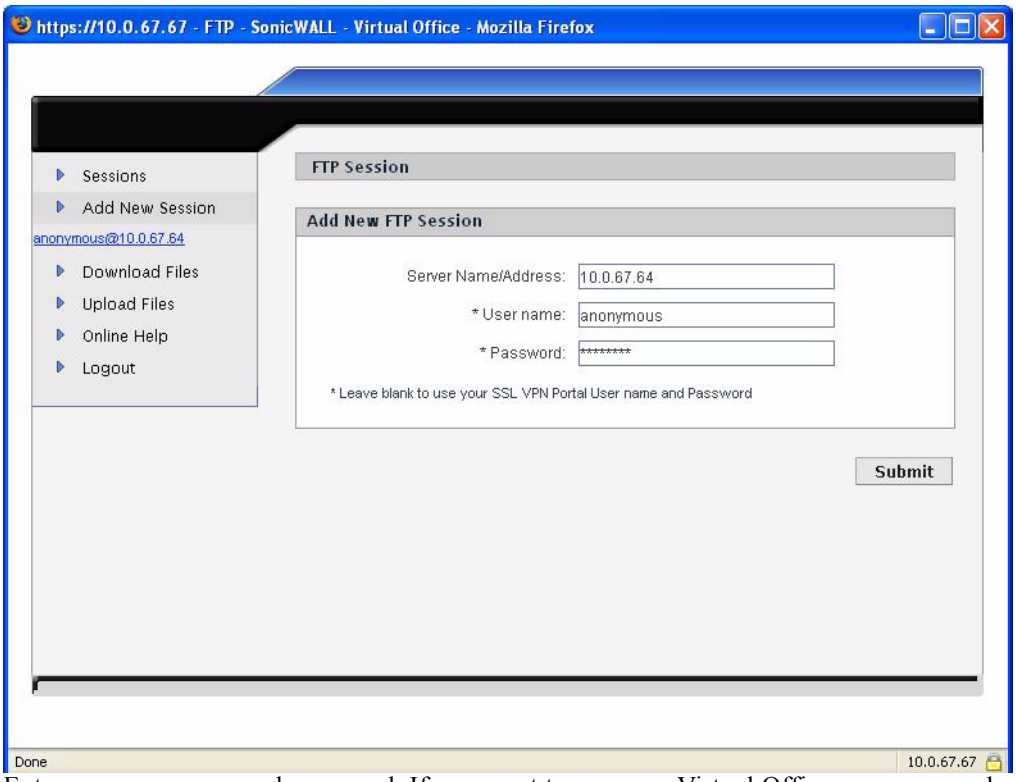
Option	Default	Description of Options
Encoding	Tight	**Hextile** is a good choice for fast networks, while **Tight** is better suited for low-bandwidth connections. From the other side, the **Tight** decoder in TightVNC Java viewer is more efficient than **Hextile** decoder so this default setting can also be acceptable for fast networks.
Compression Level	Default	Use specified compression level for **Tight** and **Zlib** encodings. Level 1 uses minimum of CPU time on the server but achieves weak compression ratios. Level 9 offers best compression but may be slow in terms of CPU time consumption on the server side. Use high levels with very slow network connections, and low levels when working over higher-speed networks. The **Default** value means that the server's default compression level should be used.
JPEG image quality	6	This cannot be modified.

Table 2 VNC Options

Option	Default	Description of Options
Cursor shape updates	Enable	Cursor shape updates is a protocol extension used to handle remote cursor movements locally on the client side, saving bandwidth and eliminating delays in mouse pointer movement. Note that current implementation of cursor shape updates does not allow a client to track mouse cursor position at the server side. This means that clients would not see mouse cursor movements if the mouse was moved either locally on the server, or by another remote VNC client. Set this parameter to **Disable** if you always want to see real cursor position on the remote side. Setting this option to **Ignore** is similar to **Enable** but the remote cursor will not be visible at all. This can be a reasonable setting if you don't care about cursor shape and don't want to see two mouse cursors, one above another.
Use CopyRect	Yes	CopyRect saves bandwidth and drawing time when parts of the remote screen are moving around. Most likely, you don't want to change this setting.
Restricted colors	No	If set to **No**, then 24-bit color format is used to represent pixel data. If set to **Yes**, then only 8 bits are used to represent each pixel. 8-bit color format can save bandwidth, but colors may look very inaccurate.
Mouse buttons 2 and 3	Normal	If set to **Reversed**, then right mouse button (button 2) will act as it was middle mouse button (button 3), and vice versa.
View only	No	If set to **Yes**, then all keyboard and mouse events in the desktop window will be silently ignored and will not be passed to the remote side.
Share desktop	Yes	If set to **Yes**, then the desktop can be shared between clients. If this option is set to **No** then an existing user session will end when a new user accesses the desktop.

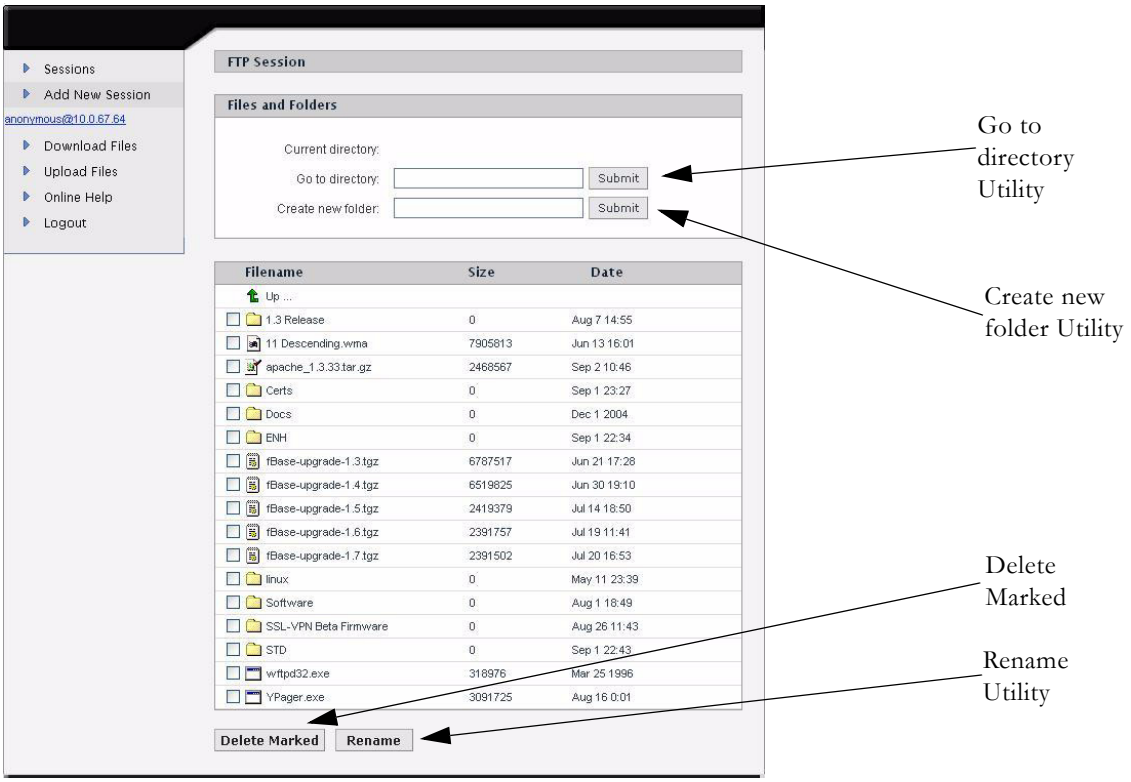
Using FTP Bookmarks

Step 1 Click the **FTP** bookmark. The **FTP Session** dialog box displays.



Step 2 Enter your username and password. If you want to use your Virtual Office username and password, simply leave the fields blank.

Step 3 Click **Submit**. An FTP session displays.



Step 4 You can use the following utilities in the FTP site:

- To manually navigate to a folder, enter the folder name in the **Go to directory** field and click **Submit**.
- To create new folders in the directory, use the **Create new folder** fields.
- To delete multiple files, click in the checkboxes of files or folders you want to remove and click **Delete Marked**.
- To rename a file or folder, click in the checkbox of a file or a folder and click **Rename**.

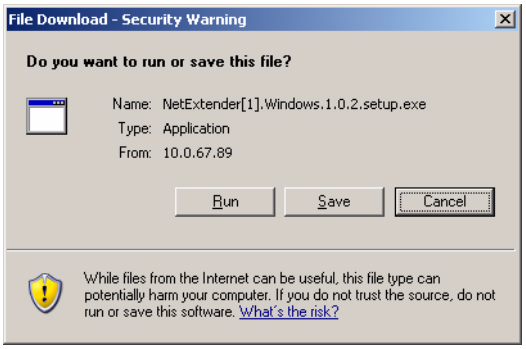
Step 5 To initiate another FTP session, click the **Add New Session** button. To return to the initial FTP session, click the link for it (in the form username@ipaddress) under the **Add New Session** button.

Downloading Files

To download a file, perform the following:

Step 1 Click **Download Files** in the navigation bar.

Step 2 Click on the name of the file in the **Filename** column. The File Download window displays.

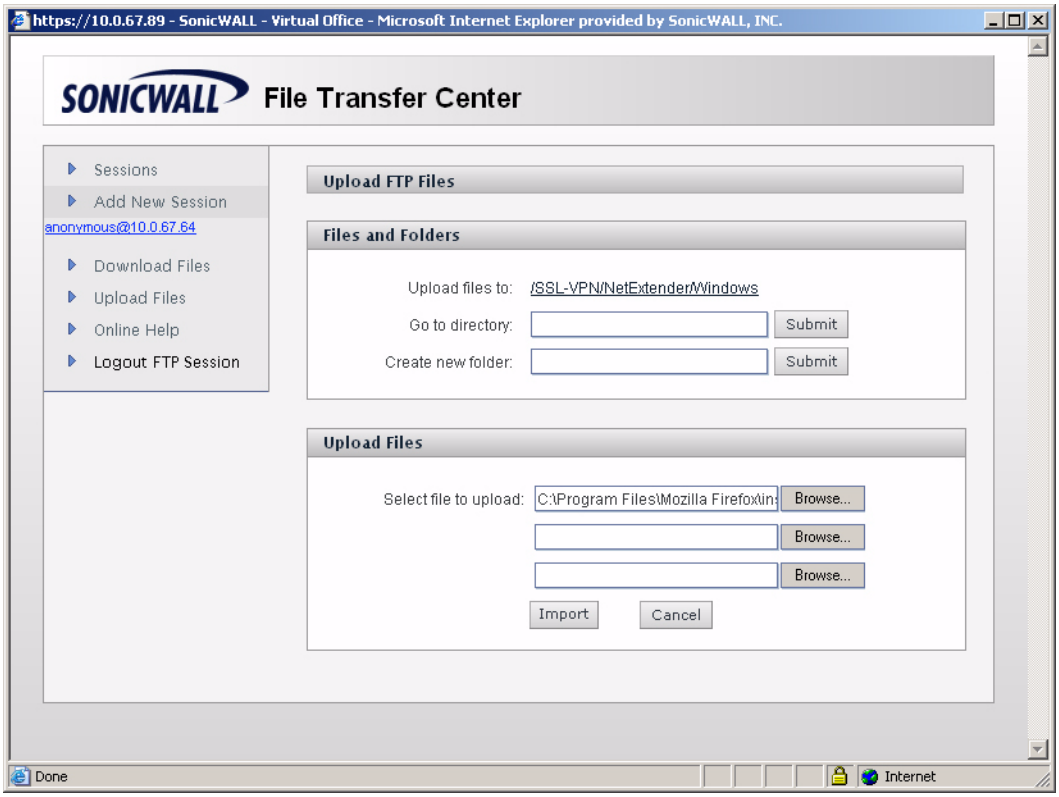

File Download - Security Warning
Do you want to run or save this file?
Name: NetExtender[1].Windows.1.0.2.setup.exe
Type: Application
From: 10.0.67.89
Run
Save
Cancel
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

Step 3 Click **Run** to launch the file. Click **Save** to save it to your computer.

Uploading Files

To upload a file, perform the following:

Step 1 Click **Upload Files** in the navigation bar. The FTP Session upload files window will be displayed.



Step 2 The current directory is displayed in the **Upload files to:** field. To navigate to a different directory, enter the directory name in the **Go to directory:** field. To create a new folder in the current directory, enter the name of the folder in the **Create new folder:** field and click submit.

Step 3 Select the file you want to upload by clicking the **Browse...** button and navigating to the file. You can upload up to three files at once.

Note To navigate between uploads, click the **Sessions** link.

Step 4 Click **Import** to upload the files.

Using Telnet Bookmarks

Step 1 Click on the Telnet bookmark.

Note Telnet bookmarks can use a port designation for servers not running on the default port.

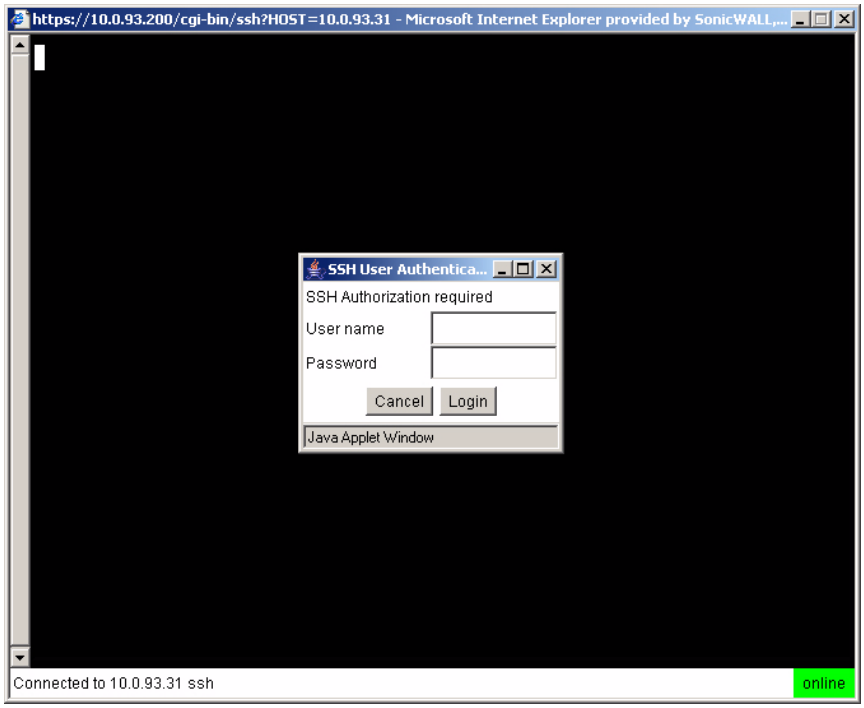
Step 2 Click **ok** to any warning messages that are displayed. A Java-based Telnet window launches.

Step 3 If the device you are Telnetting to is configured for authentication, enter you username and password.

Using SSHv1 Bookmarks

Step 1 Click on the SSHv1 bookmark. A Java-based SSH window is launched.

Note SSH bookmarks can use a port designation for servers not running on the default port.



Step 2 Enter your username and password.

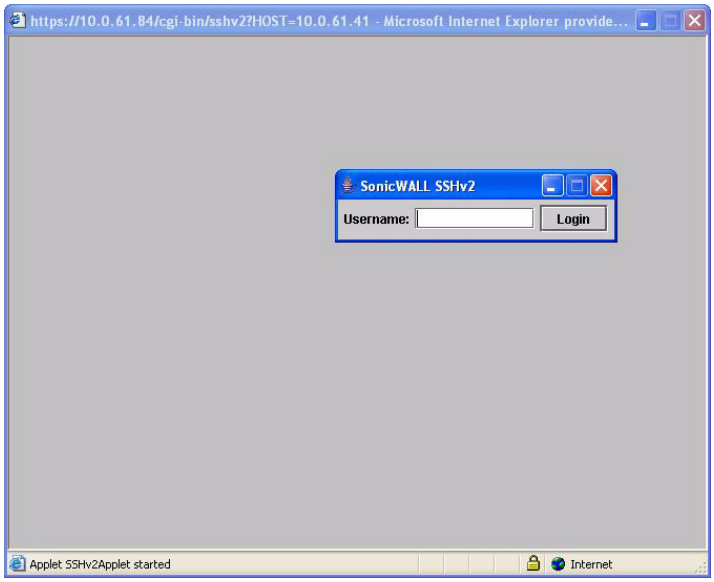
Step 3 A SSH session is launched in the Java applet.

Tip Some versions of JRE may cause the SSH authentication window to pop up behind the SSH window.

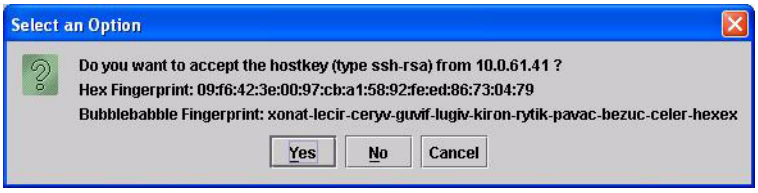
Using SSHv2 Bookmarks

Step 1 Click on the SSHv2 bookmark. A Java -based SSH window displays. Type your user name in the **Username** field and click **Login**.

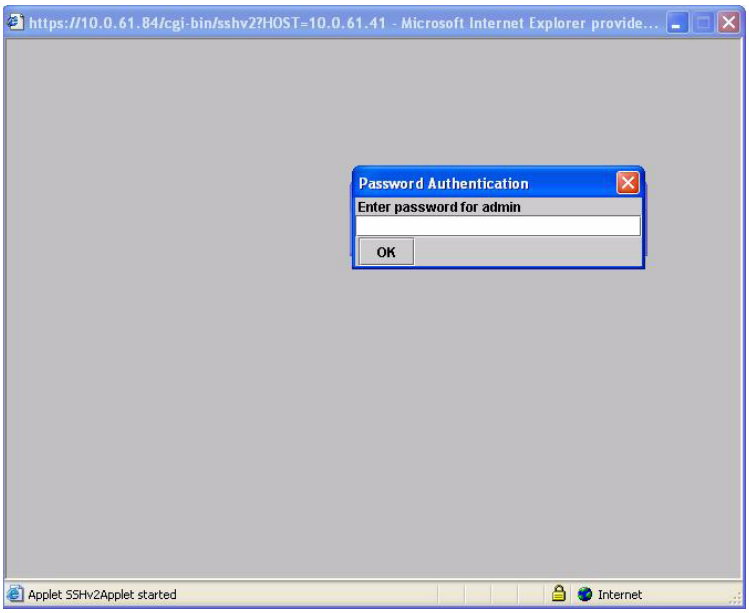
Note SSH bookmarks can use a port designation for servers not running on the default port.



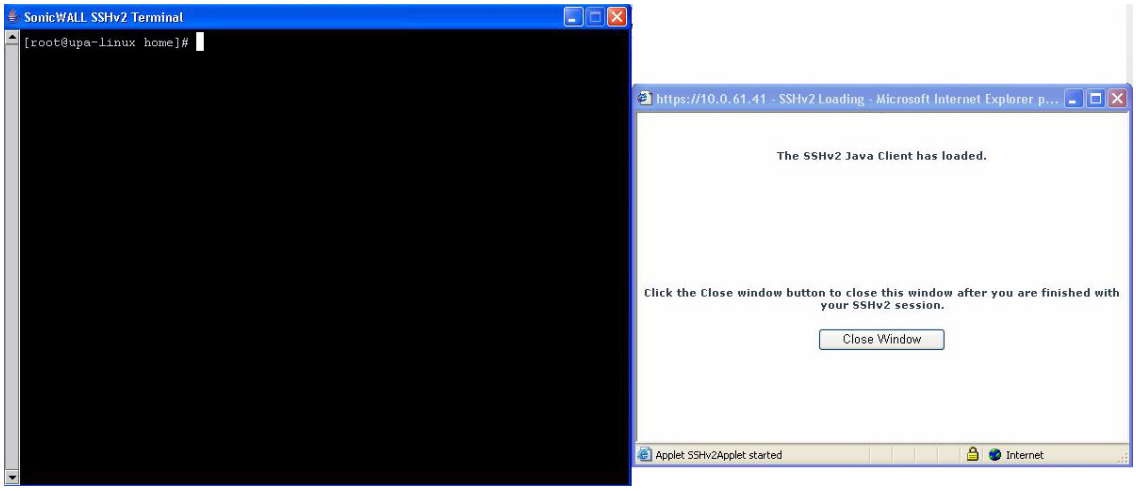
Step 2 A hostkey popup displays. Click **Yes** to accept and proceed with the login process.



Step 3 Enter your password and click **OK**.



Step 4 The SSH terminal launches in a new screen.


SonicWALL SSHv2 Terminal
[root@upa-linux home]#
https://10.0.61.41 - SSHv2 Loading - Microsoft Internet Explorer p...
The SSHv2 Java Client has loaded.
Click the Close window button to close this window after you are finished with your SSHv2 session.
Close Window
Applet SSHv2Applet started
Internet

Using HTTP and HTTPS Bookmarks

Step 1 Click on the HTTP or HTTPS bookmark.

Note HTTP bookmarks can have a port designation and a path.

Step 2 A new window is launched in your default browser that connects to the domain name or IP address specified in the bookmark.

Note OWA Premium and Lotus Domino Web Access are supported in SSL-VPN 2.0. Other applications may work but there may be problems accessing pages that are malformed, have advanced HTML features, use an unsupported authentication method (for example, Windows Integrated Authentication) and URLs that are embedded in Macromedia Flash, Java or ActiveX.

Using File Share Bookmarks

For information on using File Share bookmarks, see the previous "Using File Shares" section on page 32.

Using Citrix Bookmarks

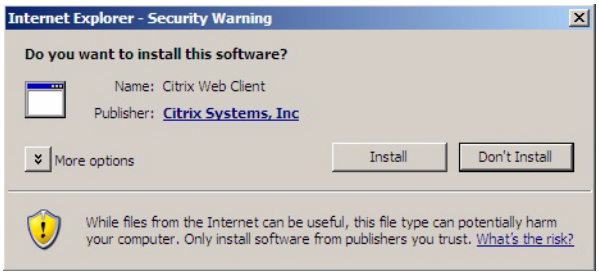
Citrix is a remote access, application sharing service, similar to RDP. It enables users to remotely access files and applications on a central computer over a secure connection.

Platforms

Note Citrix is supported on the SonicWALL SSL-VPN 2000 and SSL-VPN 4000 security appliances.

Step 1 Click on the Citrix bookmark.

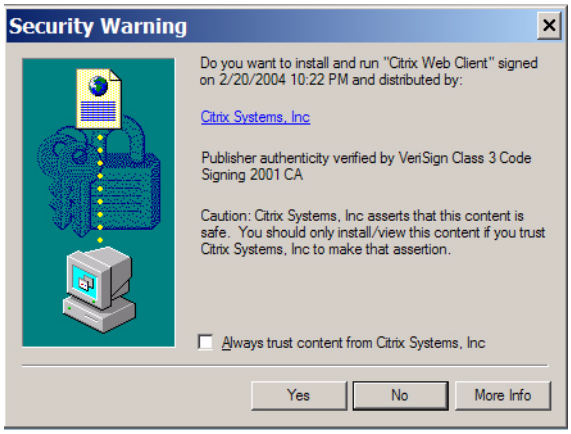
Step 2 The first time you use a Citrix bookmark, it will install the Citrix Web Client on your computer. Click **Install** to install the client.


Internet Explorer - Security Warning
Do you want to install this software?
Name: Citrix Web Client
Publisher: Citrix Systems, Inc
More options
Install
Don't Install
While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

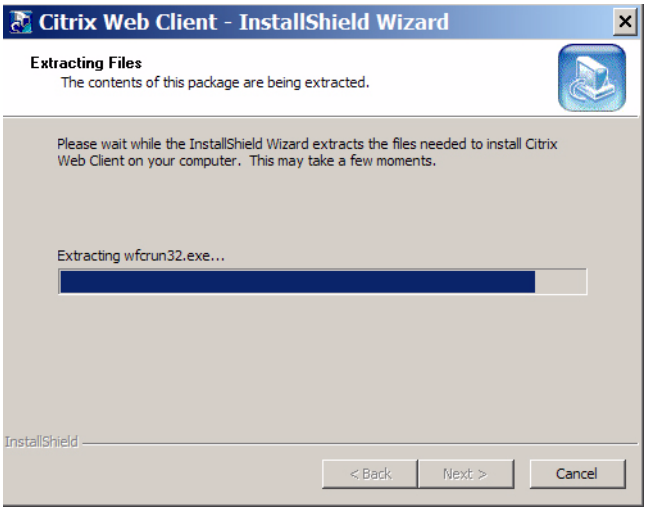
Step 3 The Citrix Web Client begins to install. If prompted, click the banner to grant ActiveX control to the Citrix Web Client.

https://10.0.61.150 - Citrix Installation - Microsoft Internet Explorer
This site might require the following ActiveX control: 'Citrix Web Client' from 'Citrix Systems, Inc'. Click here to install...
Please wait while the Citrix Web Client is installed ...
After installation, you will be automatically redirected to the Citrix portal

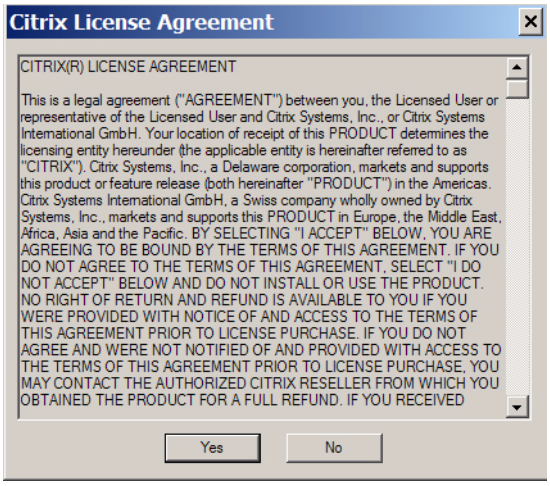
Step 4 Click **Yes** to the Security Warning message that is displayed.


Security Warning
Do you want to install and run "Citrix Web Client" signed on 2/20/2004 10:22 PM and distributed by:
Citrix Systems, Inc
Publisher authenticity verified by VeriSign Class 3 Code Signing 2001 CA
Caution: Citrix Systems, Inc asserts that this content is safe. You should only install/view this content if you trust Citrix Systems, Inc to make that assertion.
Always trust content from Citrix Systems, Inc
Yes
No
More Info

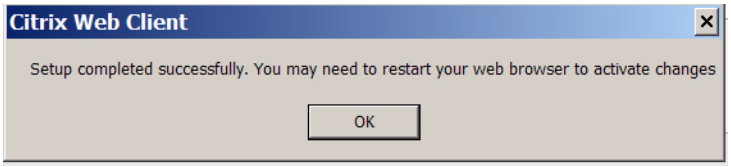
Step 5 The Citrix Web Client installs.


Citrix Web Client - InstallShield Wizard
Extracting Files
The contents of this package are being extracted.
Please wait while the InstallShield Wizard extracts the files needed to install Citrix Web Client on your computer. This may take a few moments.
Extracting wfcrun32.exe...
InstallShield
< Back
Next >
Cancel

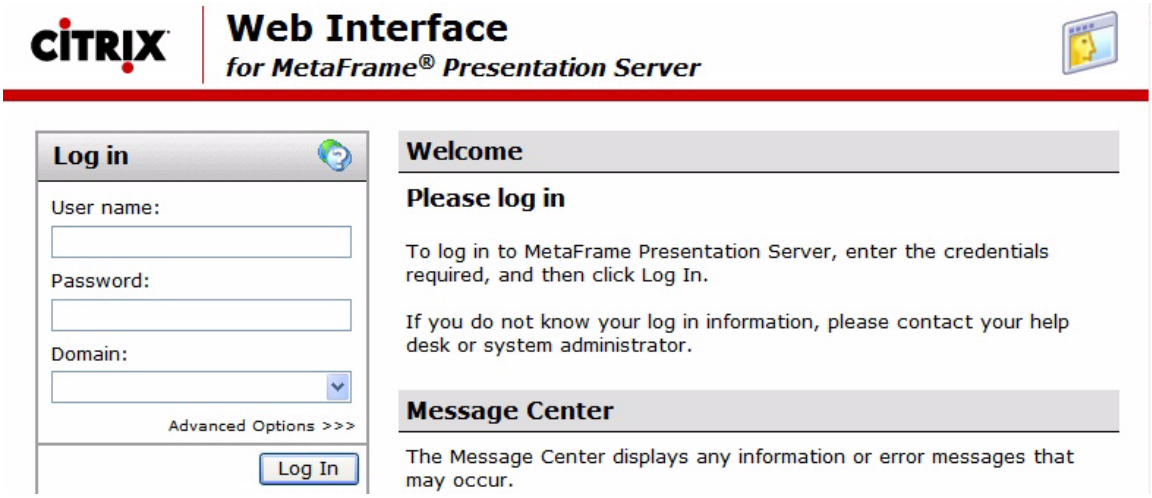
Step 6 Click **Yes** to the Citrix license agreement.


Citrix License Agreement
CITRIX(R) LICENSE AGREEMENT
This is a legal agreement ("AGREEMENT") between you, the Licensed User or representative of the Licensed User and Citrix Systems, Inc., or Citrix Systems International GmbH. Your location of receipt of this PRODUCT determines the licensing entity hereunder (the applicable entity is hereinafter referred to as "CITRIX"). Citrix Systems, Inc., a Delaware corporation, markets and supports this product or feature release (both hereinafter "PRODUCT") in the Americas. Citrix Systems International GmbH, a Swiss company wholly owned by Citrix Systems, Inc., markets and supports this PRODUCT in Europe, the Middle East, Africa, Asia and the Pacific. BY SELECTING "I ACCEPT" BELOW, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, SELECT "I DO NOT ACCEPT" BELOW AND DO NOT INSTALL OR USE THE PRODUCT. NO RIGHT OF RETURN AND REFUND IS AVAILABLE TO YOU IF YOU WERE PROVIDED WITH NOTICE OF AND ACCESS TO THE TERMS OF THIS AGREEMENT PRIOR TO LICENSE PURCHASE. IF YOU DO NOT AGREE AND WERE NOT NOTIFIED OF AND PROVIDED WITH ACCESS TO THE TERMS OF THIS AGREEMENT PRIOR TO LICENSE PURCHASE, YOU MAY CONTACT THE AUTHORIZED CITRIX RESELLER FROM WHICH YOU OBTAINED THE PRODUCT FOR A FULL REFUND. IF YOU RECEIVED
Yes
No

Step 7 When the Citrix Web Client has installed, click **Ok**. If the Citrix MetaFrame XP login window does not display, restart your web browser and launch the Citrix bookmark again.

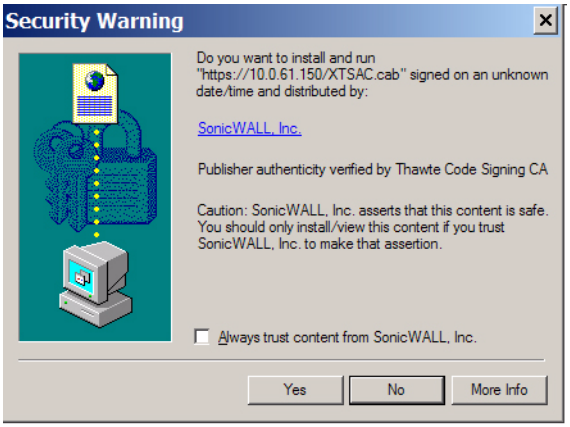


Step 8 Enter your username, password, and domain in the Citrix MetaFrame XP login window.

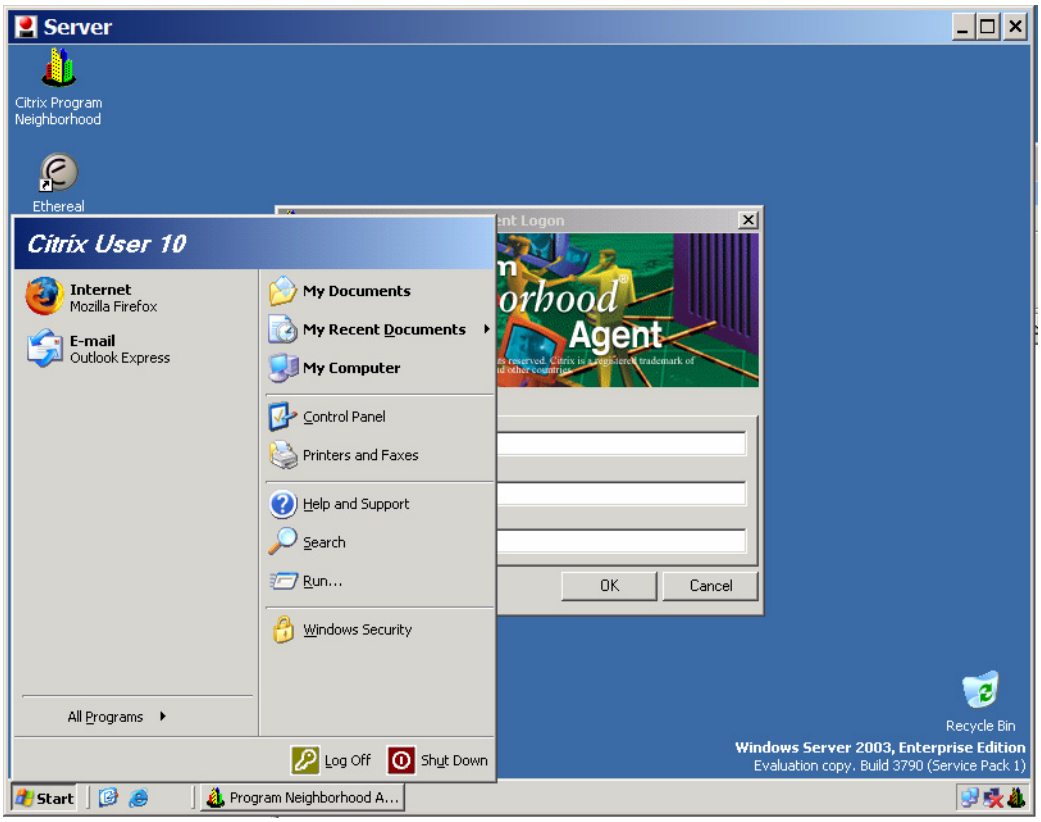

CITRIX
Web Interface
for MetaFrame® Presentation Server
Log in
User name:
Password:
Domain:
Advanced Options >>>
Log In
Welcome
Please log in
To log in to MetaFrame Presentation Server, enter the credentials required, and then click Log In.
If you do not know your log in information, please contact your help desk or system administrator.
Message Center
The Message Center displays any information or error messages that may occur.

Step 9 The Citrix MetaFrame XP home page is displayed. Click on the application you want to use.

Step 10 You may be prompted to install additional Citrix software.


Security Warning
Do you want to install and run "https://10.0.61.150/XTSAC.cab" signed on an unknown date/time and distributed by:
SonicWALL, Inc.
Publisher authenticity verified by Thawte Code Signing CA
Caution: SonicWALL, Inc. asserts that this content is safe. You should only install/view this content if you trust SonicWALL, Inc. to make that assertion.
Always trust content from SonicWALL, Inc.
Yes
No
More Info

Step 11 The shared application is now launched.



Logging Out of the Virtual Office

To end your session, simply return to the Virtual Office home page from wherever you are within the portal and click on the Logout button.

SONICWALL Virtual Office
Welcome, joe user!
Logout
Help
Welcome to the SSL-VPN 2000
SonicWALL Virtual Office provides secure Internet access for remote users to log in and access private network resources via SSL-VPN technology.
Click a pre-configured bookmark or create your own to gain secure Internet access to internal corporate resources.
Launch NetExtender to create an SSL-VPN tunnel to your corporate network for full network access.
NetExtender
Help >>
File Shares
Help >>
Logout Button

If you have successfully logged out, the system collapses the window and displays the text:

User successfully logged out. Close this window.

Note When using the Virtual Office with the **admin** username, the **Logout** button is not displayed. This is a security measure to ensure that administrators log out of the administrative interface, and not the Virtual Office.

Trademarks

SonicWALL is a registered trademark of SonicWALL, Inc.

Microsoft Windows 98, Windows NT, Windows 2000, Windows XP, Windows Server 2003, Internet Explorer, and Active Directory are trademarks or registered trademarks of Microsoft Corporation.

Netscape is a registered trademark of Netscape Communications Corporation in the U.S. and other countries. Netscape Navigator and Netscape Communicator are also trademarks of Netscape Communications Corporation and may be registered outside the U.S.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the U.S. and/or other countries.

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Limited Warranty

SonicWALL, Inc. warrants that commencing from the delivery date to Customer (but in any case commencing not more than ninety (90) days after the original shipment by SonicWALL), and continuing for a period of twelve (12) months, that the product will be free from defects in materials and workmanship under normal use. This Limited Warranty is not transferable and applies only to the original end user of the product. SonicWALL and its suppliers' entire liability and Customer's sole and exclusive remedy under this limited warranty will be shipment of a replacement product. At SonicWALL's discretion the replacement product may be of equal or greater functionality and may be of either new or like-new quality. SonicWALL's obligations under this warranty are contingent upon the

return of the defective product according to the terms of SonicWALL's then-current Support Services policies.

This warranty does not apply if the product has been subjected to abnormal electrical stress, damaged by accident, abuse, misuse or misapplication, or has been modified without the written permission of SonicWALL.

DISCLAIMER OF WARRANTY. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE MAXIMUM EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

Index

B
bookmarks 12, 34, 35
  adding 35
  description 12
  overview 34
  removing 38
bookmarks list 38
D
disconnect option 29
domains 34
downloading files
  FTP 46
F
file shares 12, 33
  desciption 12
FTP
  session 45
    password 44
  session dialog box 44
H
home page
  Virtual Office 12, 13
L
local groups 34
local users 34
logging in 11, 12
logging out 55
login page 11
N
NetExtender 10, 12, 13, 15, 19, 21, 22, 24
  description 12
  exting the browser 29
  route information 30
  status fields 21
  status window 21, 24
  system tray 22, 29
P
portal 15, 55
R
RDP bookmarks 40
remote desktop 40
S
services 35
SonicWALL technical support 7
SSL 9, 13, 15, 18
SSL-VPN 5, 8, 9, 10, 11, 13, 15, 18, 32, 34
SSL-VPN access features 13
T
Terminal Server 40
U
uploading files 46
  FTP 46
V
Virtual Office 9, 11, 12
  environments supported 13
  features 15
  home page 12, 13
  logging out 55

SonicWALL, Inc.
1143 Borregas Avenue
Sunnyvale CA 94089-1306

T +1 408.745.9600
F +1 408.745.9300

www.sonicwall.com

SONICWALL®

PN: 232-000756-00 Rev A

©2006 SonicWALL, Inc. is a registered trademark of SonicWALL, Inc. Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.
Specifications and descriptions subject to change without notice.